



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549  
FORT MEADE, MARYLAND 20755-0549

IN REPLY  
REFER TO: Joint Interoperability Test Command (JTE)

1 Jun 12

### MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Microsoft® Lync™ Server 2010 with Software Release 4.0.279

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004  
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008  
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.
2. The Microsoft® Lync™ Server 2010 with software release 4.0.279 is hereinafter referred to as the System Under Test (SUT). The SUT is certified for joint use in the Defense Information System Network as an Extensible Messaging and Presence Protocol (XMPP) Gateway. The Defense Information Systems Agency (DISA) adjudicated all Test Discrepancy Reports (TDR) open at the completion of testing to have a minor operational impact. The fielding of the SUT is limited to Internet Protocol version 4 (IPv4) only. The SUT did not support Internet Protocol version 6 (IPv6) at the time of their test window; however, the vendor has submitted a Plan of Actions and Milestones (POA&M) to demonstrate IPV6 capability before the end of August 2012. The certification status of the SUT will be evaluated for any new discrepancies noted in the operational environment for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor's POA&M that addresses all new critical TDRs within 120 days of identification. JITC conducted testing using XMPP requirements derived from the Unified Capabilities Requirements (UCR) 2008, Change 3, Reference (c) and using test procedures derived from Reference (d). JITC does not certify any other configurations, features, or functions, except those cited within this memorandum. This certification expires upon changes that could affect interoperability, but no later than three years from the date of the Unified Capabilities (UC) Approved Products List (APL) memorandum.
3. This finding is based on interoperability testing, review of the vendor's Letters of Compliance (LoC), DISA adjudication of open TDRs, and DISA Certification Authority (CA) positive recommendation of the Information Assurance configuration. JITC conducted interoperability testing at the Fort Huachuca Global Information Grid Network Test Facility from 4 through 16 December 2011. Review of the vendor's LoC was completed on 16 December 2011. DISA adjudication of open TDRs was completed on 7 February 2012. The DISA CA provided a positive Recommendation on 1 June 2012 based on the security testing completed by DISA-led

IA test teams and published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations.

4. Section 5.7.3 of the UCR establishes the interfaces and threshold CRs/FRs used to evaluate the interoperability of the SUT. The SUT was tested specifically as an XMPP gateway and not as an XMPP client/server system. Tables 1 and 2 list the interface and CR/FR interoperability status of the SUT. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

**Table 1. SUT Interface Interoperability Status**

| Interface    | Critical <sup>1</sup> | UCR Reference                    | Threshold CRs/FRs <sup>2</sup> | Criteria                                      | Status     |
|--------------|-----------------------|----------------------------------|--------------------------------|---|------------|
| IEEE 802.3i  | No                    | UCR 2008 Change 3, section 5.3.1 | 1-15                           | Meet minimum CR/FRs and IEEE 802.3 standards. | Not Tested |
| IEEE 802.3u  | No                    |                                  | 1-15                           |   | Certified  |
| IEEE 802.3z  | No                    |                                  | 1-15                           |   | Not Tested |
| IEEE 802.3ab | No                    |                                  | 1-15                           |   | Certified  |

**NOTES:**

1. The UCR does not specify minimum required interfaces for an XMPP gateway; however, the SUT must provide at least one for connectivity to an ASLAN.

2. The SUT’s specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2.

**LEGEND:**

|         |                                     |      |   |
|---------|-------------------------------------|------|---|
| 802.3i  | 10 Mbps copper Ethernet             | IA   | Information Assurance                             |
| 802.3u  | 100 Mbps copper/fiber Ethernet      | ID   | Identification                                    |
| 802.3z  | 1000 Mbps fiber Ethernet            | IEEE | Institute of Electrical and Electronics Engineers |
| 802.3ab | 1000 Mbps Copper Ethernet           | Mbps | Megabits per second                               |
| ASLAN   | Assured Services Local Area Network | SUT  | System Under Test                                 |
| CR      | Capability Requirements             | UCR  | Unified Capabilities Requirements                 |
| FR      | Functional Requirements             | XMPP | Extensible Messaging and Presence Protocol        |

**Table 2. SUT Capability Requirements and Functional Requirements Status**

| CR/FR ID   | Capability/ Function                            | Applicability (See note 1.) | UCR 2008 Change 3 Reference | Status                     |
|--|---|-----------------------------|-----------------------------|----------------------------|
| <b>Extensible Messaging and Presence Protocol (XMPP)</b> |   |                             |                             |                            |
| <b>1</b>   | XML Streams                                     | Required                    | 5.7.3.7                     | Met                        |
| <b>2</b>   | TLS and STARTTLS Negotiation                    | Required                    | 5.7.3.8                     | Met                        |
| <b>3</b>   | Authentication and SASL Negotiation             | Required                    | 5.7.3.9                     | Met                        |
| <b>4</b>   | Resource Binding                                | Required                    | 5.7.3.10                    | Met                        |
| <b>5</b>   | XML Stanzas                                     | Required                    | 5.7.3.11                    | Met                        |
| <b>6</b>   | Roster Management                               | Required                    | 5.7.3.12                    | Partially Met <sup>2</sup> |
| <b>7</b>   | Presence Subscription Management                | Required                    | 5.7.3.13                    | Partially Met <sup>2</sup> |
| <b>8</b>   | Exchanging Presence Information                 | Required                    | 5.7.3.14                    | Met                        |
| <b>9</b>   | Exchanging Messages                             | Required                    | 5.7.3.15                    | Met                        |
| <b>10</b>  | Conformance Requirements in RFC6120 and RFC6121 | Required                    | 5.7.3.16                    | Met                        |
| <b>11</b>  | XMPP Extensions                                 | Required                    | 5.7.3.17                    | Partially Met <sup>3</sup> |
| <b>12</b>  | XML Usage                                       | Required                    | 5.7.3.18                    | Met                        |
| <b>13</b>  | DSCP Requirements                               | Required                    | 5.7.3.19                    | Met                        |

**Table 2. SUT Capability Requirements and Functional Requirements Status (continued)**

| CR/FR ID                                 | Capability/ Function   | Applicability (See note 1.) | UCR 2008 Change 3 Reference | Status               |
|--|--|-----------------------------|-----------------------------|----------------------|
| Internet Protocol Version 6 Requirements |  |                             |                             |                      |
| 14                                       | IPv6   | Required                    | 5.3.5                       | Not Met <sup>4</sup> |
| Information Assurance Requirements       |  |                             |                             |                      |
| 15                                       | Detailed requirements and associated criteria for XMPP are listed Reference (e). | Required                    | 5.4.6.2                     | Met <sup>5</sup>     |

**NOTES:**

1. The annotation of ‘required’ refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.

2. Presence of the Microsoft client is sent to users who are no longer contacts. The mitigation for removal of contact and presence updates is a two-step process: Block contact and then remove the contact to prevent presence information from being sent after deletion. This anomaly was adjudicated by DISA on 7 February 2012 as having a minor impact with the stipulation that the vendor insert these mitigation instructions in the SUT Deployment Guide.

3. The SUT does not support extensions associated with Multi-User Chat (MUC). Since XMPP gateways are not required to support MUC, there is no operational impact.

4. The SUT is not IPv6 capable and does not support traffic class tagging for IPv6 XMPP packets. DISA adjudicated this as having a minor operational impact based on the vendor’s POA&M stating that IPv6 will be supported in August 2012. The vendor must bring the SUT in for IPv6 verification and validation testing in August 2012 or the SUT is subject to removal from the UC APL.

5. Security is tested by a DISA-led IA test team and published in a separate report, Reference (e).

**LEGEND:**

|       |                                    |          |  |
|-------|------------------------------------|----------|--|
| APL   | Approved Products List             | SASL     | Simple Authentication and Security Layer     |
| CR    | Capability Requirement             | SSL      | Secure Socket Layer                          |
| DISA  | Defense Information Systems Agency | STARTTLS | name of the operation for initiating TLS/SSL |
| DSCP  | Differential Service Code Point    | SUT      | System Under Test                            |
| FR    | Functional Requirement             | TLS      | Transport Layer Security                     |
| IA    | Information Assurance              | UC       | Unified Capabilities                         |
| ID    | Identification                     | UCR      | Unified Capabilities Requirements            |
| IPv6  | Internet Protocol version 6        | XML      | Extensible Mark-up Language                  |
| POA&M | Plan of Actions and Milestones     | XMPP     | Extensible Messaging and Presence Protocol   |
| RFC   | Request For Comments               |          |  |


5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: [ucco@disa.mil](mailto:ucco@disa.mil).

JITC Memo, JTE, Special Interoperability Test Certification of the Microsoft® Lync™ Server 2010 with Software Release 4.0.279

6. The JITC point of contact is Mr. Cary Hogan, DSN 879-2589, commercial (520) 538-2589, FAX DSN 879-4347, or e-mail to cary.v.hogan.civ@mail.mil . The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 1129701.

FOR THE COMMANDER:

3 Enclosures a/s

  
for RICHARD A. MEADOR  
Chief  
Battlespace Communications Portfolio

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT),  
SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities  
Division, J68

Defense Information Systems Agency, GS23

## **ADDITIONAL REFERENCES**

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 2," 31 December 2010
- (d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)," Draft
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of Microsoft Lync Extensible Messaging and Presence Protocol (XMPP) (Tracking Number 1129701)," Draft

## CERTIFICATION TESTING SUMMARY

**1. SYSTEM TITLE.** Microsoft® Lync™ Server 2010 with Software Release 4.0.279; hereinafter referred to as the System Under Test (SUT).

**2. SPONSOR.** Ms. Catrena Gainer, Defense Information Systems Agency (DISA), NS231, 6916 Cooper Avenue, Fort Meade, Maryland, 20755-7901, email: catrena.gainer@disa.mil.

**3. SYSTEM POC.** Mr. Martin Isaksen, Microsoft Federal, 5404 Wisconsin Avenue Suite 700, Chevy Chase, Maryland 20815, misaksen@microsoft.com.

**4. TESTER.** Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

**5. SYSTEM DESCRIPTION.** The SUT is an Extensible Messaging and Presence Protocol (XMPP) gateway. The SUT is comprised of an XMPP gateway with additional virtual components on the physical host. The SUT was tested specifically as an XMPP gateway and not as an XMPP client/server system. The SUT components are listed below.

**LABRAT2.** The physical host server running Microsoft Windows Server 2008R2, Hyper-V virtualization software.

**LXMPP-GW.** Provides XMPP to Session Initiation Protocol (SIP) gateway functionality. Provides Instant Messaging (IM) & Presence (P) data to XMPP clients outside of the system.

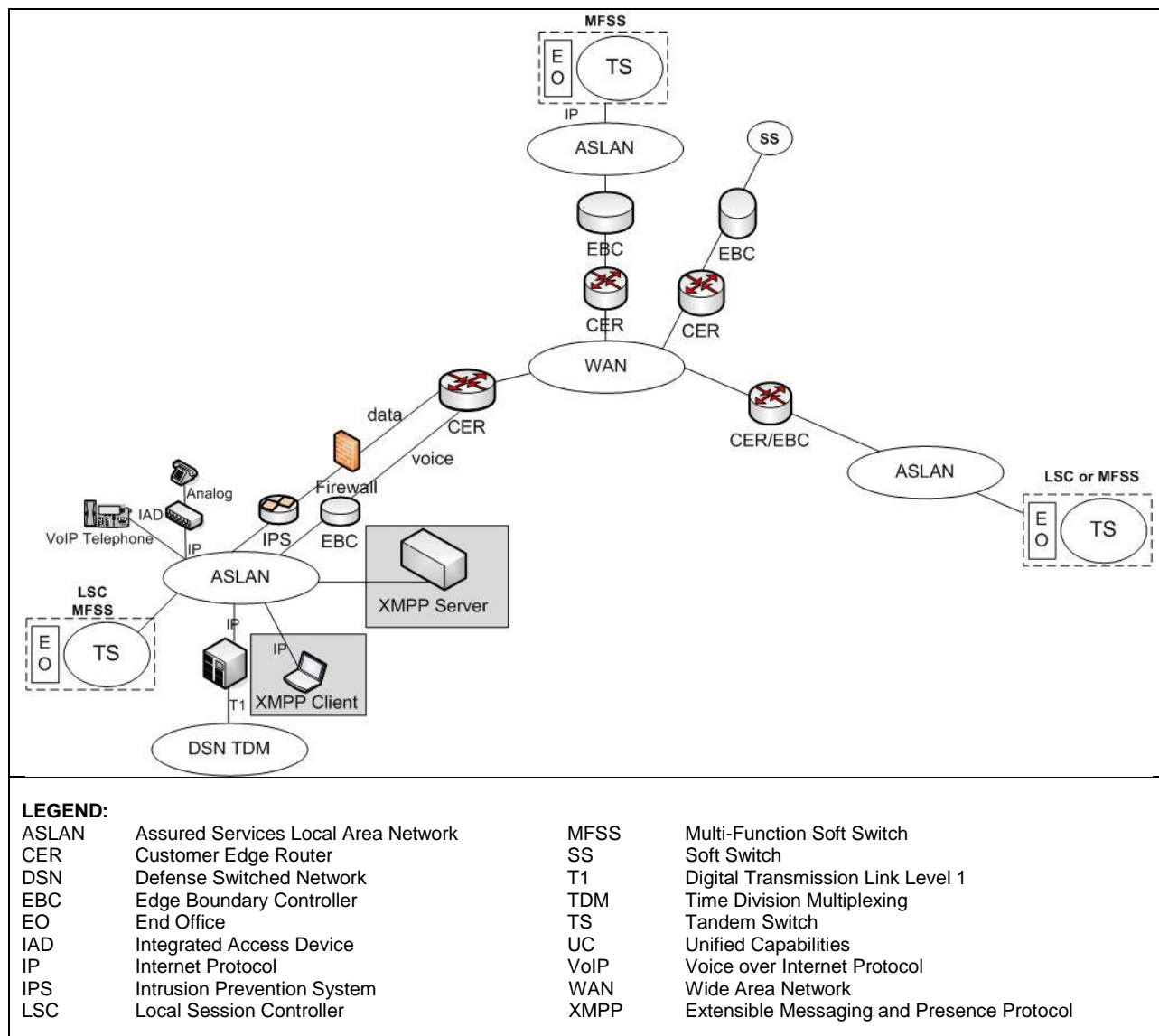
**LXMPP-SE.** The SUT SIP Session Controller. Acts as a SIP registrar and session controller. It also stores presence and contact information for endpoints.

**LXMPP-EDGE.** The SUT external access proxy server. Allows external and federated users to connect to internal accounts and users.

**LXMPP-AD.** The SUT Virtual Active Directory Server. Provides directory and authentication for the system under test.

**LXMPP-WIN7.** Client workstation running Lync 2010 IM and P client. Lync is the client endpoint for all SUT Unified Capabilities (UC) operations.

**6. OPERATIONAL ARCHITECTURE.** Figure 2-1 depicts the Defense Information System Network (DISN) Unified Capabilities notional operational architecture in which the SUT may be used.



**Figure 2. UC Architecture**

**7. INTEROPERABILITY REQUIREMENTS.** The interface, Capability Requirements (CR) and Functional Requirements (FR), Information Assurance (IA), and other requirements for XMPP are established by Section 5.7.3 of Reference (c).

**7.1 Interfaces.** The SUT uses the interfaces shown in Table 2-1 to connect to the Global Information Grid (GIG) network. This table shows the physical interfaces supported by the SUT and the associated standards.

**Table 2-1. SUT Interface Interoperability Status**

| Interface   | Critical <sup>1</sup>               | UCR Reference                          | Threshold CRs/FRs <sup>2</sup> | Criteria  |
|---|-------------------------------------|--|--------------------------------|---|
| IEEE 802.3i   | No                                  | UCR 2008<br>Change 3,<br>section 5.3.1 | 1-15                           | Meet minimum CR/FRs and IEEE 802.3 standards.     |
| IEEE 802.3u   | No                                  |  | 1-15                           |   |
| IEEE 802.3z   | No                                  |  | 1-15                           |   |
| IEEE 802.3ab  | No                                  |  | 1-15                           |   |
| <b>NOTES:</b><br>1. The UCR does not specify minimum required interfaces for an XMPP gateway; however, the SUT must provide at least one for connectivity to an ASLAN.<br>2. The SUT's specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2-2. |                                     |  |                                |   |
| <b>LEGEND:</b>  |                                     |  |                                |   |
| 802.3i  | 10 Mbps copper Ethernet             |  | IA                             | Information Assurance                             |
| 802.3u  | 100 Mbps copper/fiber Ethernet      |  | ID                             | Identification                                    |
| 802.3z  | 1000 Mbps fiber Ethernet            |  | IEEE                           | Institute of Electrical and Electronics Engineers |
| 802.3ab   | 1000 Mbps Copper Ethernet           |  | Mbps                           | Megabits per second                               |
| ASLAN   | Assured Services Local Area Network |  | SUT                            | System Under Test                                 |
| CR  | Capability Requirements             |  | UCR                            | Unified Capabilities Requirements                 |
| FR  | Functional Requirements             |  | XMPP                           | Extensible Messaging and Presence Protocol        |

**7.2 Capability Requirements (CR) and Functional Requirements (FR).** XMPP has required and conditional features and capabilities that are established by Section 5.7.3 of the UCR. The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements. The SUT's features and capabilities and its aggregated requirements in accordance with the UCR XMPP requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of Enclosure 3.

**Table 2-2. SUT Capability Requirements and Functional Requirements**

| CR/FR ID   | Capability/ Function                            | Applicability (See note.) | UCR 2008 Change 3 Reference |
|--|---|---------------------------|-----------------------------|
| <b>Extensible Messaging and Presence Protocol (XMPP)</b> |   |                           |                             |
| <b>1</b>   | XML Streams                                     | Required                  | 5.7.3.7                     |
| <b>2</b>   | TLS and STARTTLS Negotiation                    | Required                  | 5.7.3.8                     |
| <b>3</b>   | Authentication and SASL Negotiation             | Required                  | 5.7.3.9                     |
| <b>4</b>   | Resource Binding                                | Required                  | 5.7.3.10                    |
| <b>5</b>   | XML Stanzas                                     | Required                  | 5.7.3.11                    |
| <b>6</b>   | Roster Management                               | Required                  | 5.7.3.12                    |
| <b>7</b>   | Presence Subscription Management                | Required                  | 5.7.3.13                    |
| <b>8</b>   | Exchanging Presence Information                 | Required                  | 5.7.3.14                    |
| <b>9</b>   | Exchanging Messages                             | Required                  | 5.7.3.15                    |
| <b>10</b>  | Conformance Requirements in RFC6120 and RFC6121 | Required                  | 5.7.3.16                    |
| <b>11</b>  | XMPP Extensions                                 | Required                  | 5.7.3.17                    |
| <b>12</b>  | XML Usage                                       | Required                  | 5.7.3.18                    |
| <b>13</b>  | DSCP Requirements                               | Required                  | 5.7.3.19                    |
| <b>Internet Protocol Version 6 Requirements</b>          |   |                           |                             |
| <b>14</b>  | IPv6  | Required                  | 5.3.5                       |

**Table 2-2. SUT Capability Requirements and Functional Requirements  
(continued)**

| CR/FR ID  | Capability/ Function  | Applicability (See note.) | UCR 2008 Change 3 Reference                  |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
|---|---|---------------------------|--|----|------------------------|-----|---------------------|------|---------------------------------|----------|--|----|------------------------|-----|-------------------|----|----------------|-----|--------------------------|------|-----------------------------|-----|-----------------------------------|-----|----------------------|-----|-----------------------------|------|--|------|--|
| <b>Information Assurance Requirements</b>   |   |                           |  |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| <b>15</b>   | Detailed requirements and associated criteria are listed Reference (e). | Required                  | 5.4.6.2                                      |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| <p><b>NOTE:</b> The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.</p> <p><b>LEGEND:</b></p> <table> <tr> <td>CR</td><td>Capability Requirement</td> <td>SSL</td><td>Secure Socket Layer</td> </tr> <tr> <td>DSCP</td><td>Differential Service Code Point</td> <td>STARTTLS</td><td>name of the operation for initiating TLS/SSL</td> </tr> <tr> <td>FR</td><td>Functional Requirement</td> <td>SUT</td><td>System Under Test</td> </tr> <tr> <td>ID</td><td>Identification</td> <td>TLS</td><td>Transport Layer Security</td> </tr> <tr> <td>IPv6</td><td>Internet Protocol version 6</td> <td>UCR</td><td>Unified Capabilities Requirements</td> </tr> <tr> <td>RFC</td><td>Request For Comments</td> <td>XML</td><td>Extensible Mark-up Language</td> </tr> <tr> <td>SASL</td><td>Simple Authentication and Security Layer</td> <td>XMPP</td><td>Extensible Messaging and Presence Protocol</td> </tr> </table> |   |                           |  | CR | Capability Requirement | SSL | Secure Socket Layer | DSCP | Differential Service Code Point | STARTTLS | name of the operation for initiating TLS/SSL | FR | Functional Requirement | SUT | System Under Test | ID | Identification | TLS | Transport Layer Security | IPv6 | Internet Protocol version 6 | UCR | Unified Capabilities Requirements | RFC | Request For Comments | XML | Extensible Mark-up Language | SASL | Simple Authentication and Security Layer | XMPP | Extensible Messaging and Presence Protocol |
| CR  | Capability Requirement  | SSL                       | Secure Socket Layer                          |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| DSCP  | Differential Service Code Point   | STARTTLS                  | name of the operation for initiating TLS/SSL |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| FR  | Functional Requirement  | SUT                       | System Under Test                            |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| ID  | Identification  | TLS                       | Transport Layer Security                     |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| IPv6  | Internet Protocol version 6   | UCR                       | Unified Capabilities Requirements            |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| RFC   | Request For Comments  | XML                       | Extensible Mark-up Language                  |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |
| SASL  | Simple Authentication and Security Layer                                | XMPP                      | Extensible Messaging and Presence Protocol   |    |                        |     |                     |      |                                 |          |  |    |                        |     |                   |    |                |     |                          |      |                             |     |                                   |     |                      |     |                             |      |  |      |  |

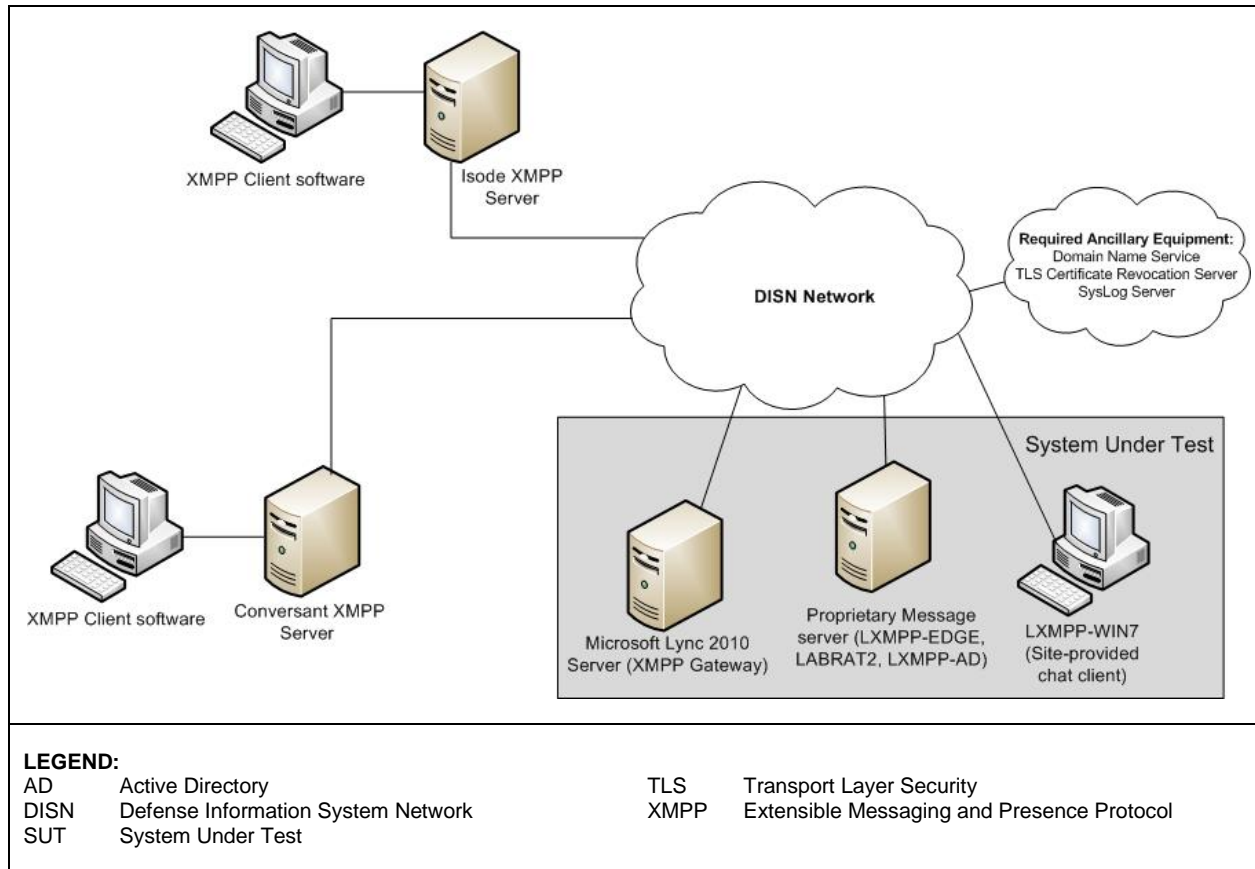
**7.3 Information Assurance.** Table 2-3 details the Information Assurance (IA) requirements applicable to the XMPP products.

**Table 2-3. XMPP IA Requirements**

| Requirement  | Applicability<br>(See note )      | UCR<br>Reference | Criteria  |
|--|-----------------------------------|------------------|---|
| General Requirements   | Required                          | 5.4.6.2          | Detailed requirements and associated<br>criteria for XMPP are listed in<br>Reference (e). |
| Authentication   | Required                          | 5.4.6.2.1        |   |
| Integrity  | Required                          | 5.4.6.2.2        |   |
| Confidentiality  | Required                          | 5.4.6.2.3        |   |
| Non-Repudiation  | Required                          | 5.4.6.2.4        |   |
| Availability   | Required                          | 5.4.6.2.5        |   |
| <b>NOTE:</b> The annotation of 'required' refers to a high-level requirement category of IA requirements from the UCR 2008, Change 3, Section 5.4. The detailed IA requirements are included in Reference (e). |                                   |                  |   |
| <b>LEGEND:</b>   |                                   |                  |   |
| IA   | Information Assurance             | XMPP             | Extensible Mark-up and Presence Protocol  |
| UCR  | Unified Capabilities Requirements |                  |   |

**7.4 Other.** None.

**8. TEST NETWORK DESCRIPTION.** The SUT was tested at the JITC, Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing the system's required functions and features was conducted using the test configuration depicted in Figure 2-2.



**Figure 2-2. SUT Test Configuration**

**9. SYSTEM CONFIGURATIONS.** Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic.

**Table 2-4. Tested System Configurations**

| Other XMPP Servers   |  | Release                                  |  |
|--|--|--|--|
| Isode M-Link   |  | R15.1v5-1                                |  |
| SoapBox XMPP Windows Server  |  | 4.3                                      |  |
|  |  | Equipment                                |  |
| Required Ancillary Equipment   |  | Domain name service                      |  |
|  |  | TLS certificate revocation server        |  |
|  |  | SysLog server                            |  |
| System Under Test<br>(See note.)   | Applications/<br>Components  | Software                                 |  |
| Microsoft® Lync™ Server 2010<br>with Software Release 4.0.279<br>on a single-unified platform            | LXMPP-GW (Provides XMPP to SIP gateway<br>functionality. Proxies IM&P data to XMPP<br>clients outside of the system.)              | Windows Server 2008R2                    |  |
|  |  | SIPXMPPTGW 3.5.6907.40                   |  |
|  |  | .NET 4.5                                 |  |
|  | LXMPP-EDGE<br>(External access proxy server. Allows<br>external and federated users to connect to<br>internal accounts and users.) | Windows Server 2008R2                    |  |
|  |  | DataProxy 4.0.7577.0                     |  |
|  |  | MediaRelaySvc 4.0.75.77.0                |  |
|  |  | MRASSvc 4.0.7577.0                       |  |
|  |  | RTCSrv 4.0.7577.0                        |  |
|  |  | .NET 4.5                                 |  |
|  |  | SQL 2008 Express                         |  |
|  | LABRAT2<br>(Physical host server.)   | Windows Server 2008R2                    |  |
|  |  | Hyper-V V6.1                             |  |
|  | LXMPP-SE<br>(SIP session controller for the SUT.)  | Windows Server 2008R2                    |  |
|  |  | OcsAppServerHost 4.0.7577.0              |  |
|  |  | FileTransferAgent 4.0.7577.0             |  |
|  |  | MasterReplicatorAgent 4.0.7577.0         |  |
|  |  | MediationServerSvc 4.0.7577.0            |  |
|  |  | ASMCUSvc 4.0.7577.0                      |  |
|  |  | IMMCUSvc 4.0.7577.139                    |  |
|  |  | MeetingMCUSvc 4.0.7577.0                 |  |
|  |  | ABServer 4.0.7577.0                      |  |
|  |  | IncomingFederation 4.0.7577.0            |  |
|  |  | MCUFactoryHost 4.0.7577.0                |  |
|  |  | RtcHost 4.0.7577.0                       |  |
|  |  | RTCSrv 4.0.7577.0                        |  |
|  |  | .NET 4.5                                 |  |
|  |  | SQL 2008 Express                         |  |
|  |  | IIS 7                                    |  |
|  | LXMPP-AD (Virtual AD server, provides<br>directory and authentication for the SUT.)  | Windows Server 2008R2                    |  |
|  |  | .NET 4.5                                 |  |
| Microsoft® Lync™ Client  | LXMPP-WIN7<br>(Site-provided client workstation)   | Windows 7                                |  |
|  |  | Lync Client 4.0.7577.275                 |  |
|  |  | Tumbleweed Desktop Validator v4.10.0.344 |  |
|  |  | ActivClient 6.2.0.50                     |  |
| <b>NOTE:</b> The SUT was tested specifically as an XMPP gateway and not as an XMPP client/server system. |  |  |  |
| <b>LEGEND:</b>   |  |  |  |
| AD   | Active Directory   | SIP                                      | Session Initiation Protocol                |
| GW   | Gateway  | SQL                                      | Structured Query Language                  |
| IIS  | Internet Information Services  | SUT                                      | System Under Test                          |
| IM&P   | Instant Messaging and Presence   | TLS                                      | Transport Layer Security                   |
| LXMPP  | Lync XMPP  | XMPP                                     | Extensible Messaging and Presence Protocol |
| SE   | Standard Edition   |  |  |

**10. TESTING LIMITATIONS.** None.

**11. INTEROPERABILITY EVALUATION RESULTS.** The SUT meets the critical interoperability requirements for XMPP in accordance with UCR 2008, Change 3,

Section 5.7.3, and is certified for joint use IPv4 only with other network infrastructure products listed on the UC APL. Additional discussion regarding specific testing results is located in subsequent paragraphs.

**11.1 Interfaces.** The interface status of the SUT is provided in Table 2-5.

**Table 2-5. SUT Interface Interoperability Status**

| Interface  | Critical <sup>1</sup>               | UCR Reference                          | Threshold CRs/FRs <sup>2</sup>                    | Criteria  | Status     |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
|--|-------------------------------------|--|---|---|------------|--------|-------------------------|----|-----------------------|--------|--------------------------------|----|----------------|--------|--------------------------|------|---|---------|---------------------------|------|---------------------|-------|-------------------------------------|-----|-------------------|----|-------------------------|-----|-----------------------------------|----|-------------------------|------|--|
| IEEE 802.3i  | No                                  | UCR 2008<br>Change 3,<br>section 5.3.1 | 1-15  | Meet minimum CR/FRs<br>and IEEE 802.3<br>standards. | Not Tested |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| IEEE 802.3u  | No                                  |  | 1-15  |   | Certified  |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| IEEE 802.3z  | No                                  |  | 1-15  |   | Not Tested |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| IEEE 802.3ab   | No                                  |  | 1-15  |   | Certified  |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| <b>NOTES:</b><br>1. The UCR does not specify minimum required interfaces for an XMPP gateway; however, the SUT must provide at least one for connectivity to an ASLAN.<br>2. The SUT's specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2-6.  |                                     |  |   |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| <b>LEGEND:</b><br><table><tr><td>802.3i</td><td>10 Mbps copper Ethernet</td><td>IA</td><td>Information Assurance</td></tr><tr><td>802.3u</td><td>100 Mbps copper/fiber Ethernet</td><td>ID</td><td>Identification</td></tr><tr><td>802.3z</td><td>1000 Mbps fiber Ethernet</td><td>IEEE</td><td>Institute of Electrical and Electronics Engineers</td></tr><tr><td>802.3ab</td><td>1000 Mbps Copper Ethernet</td><td>Mbps</td><td>Megabits per second</td></tr><tr><td>ASLAN</td><td>Assured Services Local Area Network</td><td>SUT</td><td>System Under Test</td></tr><tr><td>CR</td><td>Capability Requirements</td><td>UCR</td><td>Unified Capabilities Requirements</td></tr><tr><td>FR</td><td>Functional Requirements</td><td>XMPP</td><td>Extensible Messaging and Presence Protocol</td></tr></table> |                                     |  |   |   |            | 802.3i | 10 Mbps copper Ethernet | IA | Information Assurance | 802.3u | 100 Mbps copper/fiber Ethernet | ID | Identification | 802.3z | 1000 Mbps fiber Ethernet | IEEE | Institute of Electrical and Electronics Engineers | 802.3ab | 1000 Mbps Copper Ethernet | Mbps | Megabits per second | ASLAN | Assured Services Local Area Network | SUT | System Under Test | CR | Capability Requirements | UCR | Unified Capabilities Requirements | FR | Functional Requirements | XMPP | Extensible Messaging and Presence Protocol |
| 802.3i   | 10 Mbps copper Ethernet             | IA                                     | Information Assurance                             |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| 802.3u   | 100 Mbps copper/fiber Ethernet      | ID                                     | Identification                                    |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| 802.3z   | 1000 Mbps fiber Ethernet            | IEEE                                   | Institute of Electrical and Electronics Engineers |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| 802.3ab  | 1000 Mbps Copper Ethernet           | Mbps                                   | Megabits per second                               |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| ASLAN  | Assured Services Local Area Network | SUT                                    | System Under Test                                 |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| CR   | Capability Requirements             | UCR                                    | Unified Capabilities Requirements                 |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |
| FR   | Functional Requirements             | XMPP                                   | Extensible Messaging and Presence Protocol        |   |            |        |                         |    |                       |        |                                |    |                |        |                          |      |   |         |                           |      |                     |       |                                     |     |                   |    |                         |     |                                   |    |                         |      |  |

**11.2 Capability Requirements (CR) and Functional Requirements (FR).** The SUT CR and FR status is depicted in Table 2-6. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

**Table 2-6. SUT Capability Requirements and Functional Requirements Status**

| CR/FR ID   | Capability/ Function                            | Applicability (See note 1.) | UCR 2008 Change 3 Reference | Status                     |
|--|---|-----------------------------|-----------------------------|----------------------------|
| <b>Extensible Messaging and Presence Protocol (XMPP)</b> |   |                             |                             |                            |
| <b>1</b>   | XML Streams                                     | Required                    | 5.7.3.7                     | Met                        |
| <b>2</b>   | TLS and STARTTLS Negotiation                    | Required                    | 5.7.3.8                     | Met                        |
| <b>3</b>   | Authentication and SASL Negotiation             | Required                    | 5.7.3.9                     | Met                        |
| <b>4</b>   | Resource Binding                                | Required                    | 5.7.3.10                    | Met                        |
| <b>5</b>   | XML Stanzas                                     | Required                    | 5.7.3.11                    | Met                        |
| <b>6</b>   | Roster Management                               | Required                    | 5.7.3.12                    | Partially Met <sup>2</sup> |
| <b>7</b>   | Presence Subscription Management                | Required                    | 5.7.3.13                    | Partially Met <sup>2</sup> |
| <b>8</b>   | Exchanging Presence Information                 | Required                    | 5.7.3.14                    | Met                        |
| <b>9</b>   | Exchanging Messages                             | Required                    | 5.7.3.15                    | Met                        |
| <b>10</b>  | Conformance Requirements in RFC6120 and RFC6121 | Required                    | 5.7.3.16                    | Met                        |
| <b>11</b>  | XMPP Extensions                                 | Required                    | 5.7.3.17                    | Partially Met <sup>3</sup> |
| <b>12</b>  | XML Usage                                       | Required                    | 5.7.3.18                    | Met                        |
| <b>13</b>  | DSCP Requirements                               | Required                    | 5.7.3.19                    | Met                        |

**Table 2-6. SUT Capability Requirements and Functional Requirements Status  
(continued)**

| CR/FR ID                                 | Capability/ Function   | Applicability (See note 1.) | UCR 2008 Change 3 Reference | Status               |
|--|--|-----------------------------|-----------------------------|----------------------|
| Internet Protocol Version 6 Requirements |  |                             |                             |                      |
| 14                                       | IPv6   | Required                    | 5.3.5                       | Not Met <sup>4</sup> |
| Information Assurance Requirements       |  |                             |                             |                      |
| 15                                       | Detailed requirements and associated criteria for XMPP are listed Reference (e). | Required                    | 5.4.6.2                     | Met <sup>5</sup>     |

**NOTES:**

1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.

2. Presence of the Microsoft client is sent to users who are no longer contacts. The mitigation for removal of contact and presence updates is a two-step process: Block contact and then remove the contact to prevent presence information from being sent after deletion. This anomaly was adjudicated by DISA on 7 February 2012 as having a minor impact with the stipulation that the vendor insert these mitigation instructions in the SUT Deployment Guide.

3. The SUT does not support extensions associated with Multi-User Chat (MUC). Since XMPP gateways are not required to support MUC, there is no operational impact.

4. The SUT is not IPv6 capable and does not support traffic class tagging for IPv6 XMPP packets. DISA adjudicated this as having a minor operational impact based on the vendor's POA&M stating that IPv6 will be supported in August 2012. The vendor must bring the SUT in for IPv6 verification and validation testing in August 2012 or the SUT is subject to removal from the UC APL.

5. Security is tested by a DISA-led IA test team and published in a separate report, Reference (e).

**LEGEND:**

|       |                                    |          |  |
|-------|------------------------------------|----------|--|
| APL   | Approved Products List             | SASL     | Simple Authentication and Security Layer     |
| CR    | Capability Requirement             | SSL      | Secure Socket Layer                          |
| DISA  | Defense Information Systems Agency | STARTTLS | name of the operation for initiating TLS/SSL |
| DSCP  | Differential Service Code Point    | SUT      | System Under Test                            |
| FR    | Functional Requirement             | TLS      | Transport Layer Security                     |
| ID    | Identification                     | UC       | Unified Capabilities                         |
| IPv6  | Internet Protocol version 6        | UCR      | Unified Capabilities Requirements            |
| POA&M | Plan of Actions and Milestones     | XML      | Extensible Mark-up Language                  |
| RFC   | Request For Comments               | XMPP     | Extensible Messaging and Presence Protocol   |

**a. Product Interface Requirements**

(1) External Interface. The UCR 2008, Change 3, Section 5.3.1, states that a device which connects to an ASLAN shall be capable of supporting auto-negotiation even when the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999. This requirement was met by the SUT with both testing and the vendor's Letters of Compliance (LoC) for the 100/1000BaseT interfaces.

(2) DSCP. The UCR 2008, Change 3, paragraph 5.7.3.18, states that XMPP client and server implementations shall class mark XMPP traffic consistent with the code point values defined for ROUTINE Low-Latency Data in accordance with UCR 2008, Change 3, Table 5.3.3-1. The SUT shall support DSCP and Traffic Class tagging for prioritized traffic. Packets shall be capable of being assigned any value from 0 to 63 for prioritization. The SUT is certified for Internet protocol version 4 (IPv4)-operation only. The system is not Internet protocol version 6 (IPv6)-capable and does not support

traffic class tagging for IPv6 XMPP packets. DISA adjudicated this as having a minor operational impact based on the vendor's Plan of Actions and Milestones (POA&M) stating that IPv6 will be supported in August 2012. The vendor must bring the SUT in for IPv6 verification and validation testing in August 2012 or the SUT is subject to removal from the UC APL.

b. XMPP Requirements

(1) Extensible Markup Language (XML) streams. The UCR 2008, Change 3, paragraph 5.7.3.7.1, states "The server initiating a Transmission Control Protocol (TCP) connection determines whether the connection will be attempted in Internet protocol version 4 (IPv4) or Internet protocol version 6 (IPv6). TCP connections will be established prior to XMPP connections are established. Name resolution shall be via the Domain Name Service (DNS)." The SUT will use DNS A records for IPv4 and AAAA records for IPv6. The SUT interacted with DNS as required for IPv4. Packet capture validated TCP connections were established as IPv4 only.

(2) Transport Level Security (TLS) and Start TLS Negotiation. The UCR 2008, Change 3, paragraph 5.7.3.8, states that the SUT shall use TLS to secure XMPP traffic. It further defines behavior to establish, close, re-establish and error handling for TLS traffic. The SUT met these requirements with both testing and the vendor's LoC.

(3) Simple Authentication and Security Layer (SASL) security. The UCR 2008, Change 3, paragraph 5.7.3.9, specifies SASL in conformance with Request For Comments (RFC) 4422. SASL shall be used and anonymous login is prohibited. SASL was used correctly during the entire test event, and it was determined anonymous login was prohibited in accordance with the requirement. The SUT met these requirements with both testing and the vendor's LoC.

(4) Resource Binding. The UCR 2008, Change 3, paragraph 5.7.3.10, defines resource binding in compliance with RFC 6120. This ensures XMPP traffic is associated with the correct resource between the server and the client. During the test event XMPP traffic was correctly bound and directed to the appropriate resource. The SUT met these requirements with both testing and the vendor's LoC.

(5) XML Stanzas. The UCR 2008, Change 3, paragraph 5.7.3.11, specifies the correct format for information stanzas in XML streams. The SUT met these requirements with both testing and the vendor's LoC.

(6) Roster management. The UCR 2008, Change 3, paragraph 5.7.3.12, specifies the behavior and interaction for roster management and presence information sharing between server to server interactions and server to client interaction. Behavior to subscribe and unsubscribe, as well as population of stanza fields and responses to requests are fully defined in these sections of the requirements. Presence information was successfully conveyed during the test window bi-directionally during the testing event. The SUT partially met these requirements with both testing and the vendor's

LoC. Presence of the Microsoft client is sent to users who are no longer contacts. The mitigation for removal of contact and presence updates is a two-step process: Block contact and then remove the contact to prevent presence information from being sent after deletion. This anomaly was adjudicated by DISA on 7 February 2012 as having a minor impact with the stipulation that the vendor insert these mitigation instructions in the SUT Deployment Guide.

(7) Presence Subscription Management. The UCR 2008, Change 3, paragraph 5.7.3.13, defines the requirements associated with presence management between client to server connections and server to server connections. Presence subscription requests and approvals were successfully conveyed during the test window and bi-directionally during the testing event other than the anomaly previously noted regarding roster management. The SUT met these requirements with both testing and the vendor's LoC.

(8) Exchanging Presence information. The UCR 2008, Change 3, paragraph 5.7.3.14, states that the SUT shall be capable of sending and receiving presence information between clients. Presence was correctly conveyed between the SUT and other clients during this test event. The SUT met these requirements with both testing and the vendor's LoC.

(9) Exchanging Messages. The UCR 2008, Change 3, paragraph 5.7.3.15, defines the format for Chat messages. The SUT correctly sent and received chat messages in one-on-one chat sessions. The SUT met these requirements with both testing and the vendor's LoC.

(10) Conformance Requirements in RFC 6120 and RFC 6121. The UCR 2008, Change 3, paragraph 5.7.3.16, specifies compliance for the above listed RFCs. The SUT met these requirements with both testing and the vendor's LoC.

(11) XMPP extensions. The UCR 2008, Change 3, paragraph 5.7.3.17, specifies compliance with additional extensions to XMPP. These extensions define expected behaviors in a Multi-User Chat (MUC) environment. Gateway devices are not required to support MUC. The SUT was unable to host a MUC. The Microsoft chat clients were unable to join a MUC hosted on another server. The Microsoft clients were able to perform one-on-one chat with remote XMPP clients. SUT partially met these requirements with both testing and the vendor's LoC.

(12) XML Usage. The UCR 2008, Change 3, paragraph 5.7.3.18, requires compliance with Section 11 of RFC 6120. The SUT met these requirements with both testing and the vendor's LoC.

(13) IPv6 Compliance. The UCR 2008, Change 3, Section 5.3.5, specifies IPv6 compliance for XMPP servers, gateways and clients. The XMPP gateway software was unable to establish any IPv6 XMPP sessions. The application software on the gateway does not support IPv6. IPv6 addresses could not be entered into the

configuration screens within the application. Further interoperability testing will be performed in future testing events to establish full IPv6 capability of the SUT. The SUT did not meet these requirements. DISA adjudicated this as having a minor operational impact based on the vendor's POA&M stating that IPv6 will be supported in August 2012. The vendor must bring the SUT in for IPv6 verification and validation testing in August 2012 or the SUT is subject to removal from the UC APL.

**11.3 IA.** Security is tested by DISA-led IA test teams and published in a separate report, Reference (e).

**11.4 Other.** None.

**12. TEST AND ANALYSIS REPORT.** No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: [ucco@disa.mil](mailto:ucco@disa.mil).

## SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The XMPP has required and conditional features and capabilities that are established by Section 5.3.7 of the Unified Capabilities Requirements (UCR) 2008, Change 3. The System Under Test (SUT) need not provide conditional requirements. If they are provided, they must function according to the specified requirements. The detailed Functional requirements (FR) and Capability Requirements for XMPP are listed in Table 3-1. Detailed Information Assurance (IA) requirements are included in Reference (e) and are not listed below.

**Table 3-1. XMPP Capability/Functional Requirements**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 1  | As XMPP is defined in this specification, an initiating entity SHALL open a TCP connection to the receiving entity before it negotiates XML streams with the receiving entity. The parties then maintain that TCP connection for as long as the XML streams are in use. [Section 3.1, RFC 3920bis-17]  | 5.7.3.7.1     | R                           |
| 2  | Because XML streams are sent over TCP, the initiating entity needs to determine the IPv4 or IPv6 address (and port) of the receiving entity's "origin domain" before it can attempt to connect to the XMPP network. [Section 3.2, rfc3920bis-17]   | 5.7.3.7.1.1   | R                           |
| 3  | The fallback process SHALL be a normal "A" or "AAAA" address record resolution to determine the IPv4 or IPv6 address of the origin domain, where the port used is the "xmpp-client" port of 5222 for client-to-server connections or the "xmpp-server" port 5269 for server-to-server connections. [Section 3.2.2, rfc3920bis-17]  | 5.7.3.7.1.3   | R                           |
| 4  | It can happen that an XMPP server goes offline while servicing TCP connections from local clients and from other servers. Because the number of such connections can be quite large, the reconnection algorithm employed by entities that seek to reconnect can have a significant impact on software and network performance. When client and server implementations attempt to reconnect because of the server going "offline," they SHALL comply with the following guidelines [Section 3.3 rfc3920bis-17]  | 5.7.3.7.1.4   | R                           |
| 5  | <p>The initiating entity SHALL initiate an XML stream by sending an initial stream header to the receiving entity.</p> <p>In response, the receiving entity SHALL send a response stream header to the initiating entity.</p> <p>After the receiving entity has sent a response stream header to the initiating entity, the receiving entity SHALL send a &lt;features/&gt; child element (prefixed by the streams namespace prefix) to the initiating entity in order to announce any conditions for continuation of the stream negotiation process. Each condition takes the form of a child element of the &lt;features/&gt; element, qualified by a namespace that is different from the streams namespace and the content namespace. The &lt;features/&gt; element can contain one child, contain multiple children, or be empty. [Section 4.2.2, rfc3920bis-17]</p> <p>For stream features that are mandatory-to-negotiate, the definition of that feature SHALL declare that the feature is always mandatory-to-negotiate (e.g., this is true of resource binding for XMPP clients) or the receiving entity SHALL explicitly flag the feature as mandatory-to-negotiate (e.g., this is done for TLS by including an empty &lt;required/&gt; element in the advertisement for the STARTTLS feature). [Section 4.2.2, rfc3920bis-17]</p> <p>If the &lt;features/&gt; element contains at least one mandatory feature, then the initiating entity SHALL continue with the stream negotiation process. An empty &lt;features/&gt; element indicates that the stream negotiation is complete and that the initiating entity is cleared to send XML stanzas. [Section 4.2.2, rfc3920bis-17]</p> | 5.7.3.7.3     | R                           |
| 6  | On successful negotiation of a feature that necessitates a stream restart, both the initiating entity and the receiving entity SHALL consider the previous stream to be replaced, but SHALL NOT terminate the underlying TCP connection; instead, the initiating entity and the receiving entity SHALL reuse the existing connection. [Section 4.2.3, rfc3920bis-17]   | 5.7.3.7.4     | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 6  | The initiating entity then SHALL send a new initial stream header to the receiving entity. [Section 4.2.3, rfc3920bis-17]   | 5.7.3.7.4     | R                           |
|    | When the receiving entity receives the new initial stream header, it SHALL generate a new stream ID (instead of reusing the old stream ID) and SHALL then send a new response stream header to the initiating entity. [Section 4.2.3, rfc3920bis-17]  |               |                             |
| 7  | The receiving entity SHALL send an updated list of stream features to the initiating entity after a stream restart. [Section 4.2.4, rfc3920bis-17]  | 5.7.3.7.5     | R                           |
|    | The receiving entity SHALL indicate completion of the stream negotiation process by sending to the initiating entity either an empty <features/> element or a <features/> element that contains only voluntary features. Once stream negotiation is complete, the initiating entity is cleared to send XML stanzas over the stream for as long as the stream is maintained by both parties. [Section 4.2.5, rfc3920bis-17]  |               |                             |
| 8  | For client-to-server sessions, a server SHALL allow a client to use “two streams over a single TCP connection.”   | 5.7.3.7.6     | R                           |
|    | For server-to-server sessions, the two server peers SHALL use two streams over two TCP connections, where one TCP connection is used for the stream in which stanzas are sent from the initiating entity to the receiving entity and the other TCP connection is used for the stream in which stanzas are sent from the receiving entity to the initiating entity. [Section 4.3, rfc3920bis-17]   |               |                             |
| 9  | Client and server implementations SHALL be capable of closing an XML stream by sending a closing </stream> tag. [Section 4.4, rfc3920bis-17]  | 5.7.3.7.7.1   | R                           |
|    | After the entity that sent the first closing stream tag receives a reciprocal closing stream tag from the other party, it SHALL terminate the underlying TCP connection or connections. [Section 4.4, rfc3920bis-17]  |               |                             |
| 10 | For client-to-server connections, it is assumed that the client knows the associated XMPP account name of the form <localpart@domain>. The client SHALL include the “from” attribute in the initial stream header it sends to the server and SHALL set the value to the associated XMPP account name of the form <localpart@domain>. [Section 4.6.1, rfc3920bis-17]   | 5.7.3.7.8.1   | R                           |
|    | For server-to-server connections, the initiating entity SHALL include the “from” attribute in the initial stream header it sends to the receiving entity and SHALL set its value to a hostname serviced by the initiating entity. [Section 4.6.1, rfc3920bis-17]  |               |                             |
|    | For both client-to-server and server-to-server connections, the initiating entity SHALL include the “to” attribute in the initial stream header that it sends to the receiving entity and SHALL set its value to a hostname that the initiating entity knows or expects the receiving entity to service. [Section 4.6.2, rfc3920bis-17]   |               |                             |
|    | For both client-to-server and server-to-server connections, the initiating entity SHALL include a “version” attribute whose value is “1.0” (or higher) in the initial stream headers it generates. [Section 4.6.5, rfc3920bis-17]   |               |                             |
| 11 | For both client-to-server and server-to-server connections, the receiving entity SHALL include the “from” attribute in the response stream header that it sends to the initiating entity and SHALL set its value to a hostname serviced by the receiving entity. [Section 4.6.1, rfc3920bis-17]   | 5.7.3.7.8.2   | R                           |
|    | For response stream headers in client-to-server communication, if the client included a “from” attribute in the initial stream header then the server SHALL include a “to” attribute in the response stream header and SHALL set its value to the bare JID specified in the “from” attribute of the initial stream header. If the client did not include a “from” attribute in the initial stream header then the server SHALL NOT include a “to” attribute in the response stream header. [Section 4.6.2, rfc3920bis-17] |               |                             |
|    | For server-to-server connections, the receiving entity SHALL include the “to” attribute in the response stream header that it sends to the initiating entity and SHALL set its value to the hostname specified in the “from” attribute of the initial stream header. [Section 4.6.2, rfc3920bis-17]   |               |                             |
|    | For both client-to-server and server-to-server connections, the receiving entity SHALL include an “id” attribute in the response stream header that it sends to the initiating entity. The “id” attribute communicates a unique identifier for the stream, called a STREAM ID. The stream “id” shall have the property of randomness. [Section 4.6.3, rfc3920bis-17]  |               |                             |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 11 | For both client-to-server and server-to-server connections, the receiving entity SHALL include a "version" attribute where the value is 1.0 (or higher) in the response stream headers it sends to the initiating entity. [Section 4.6.5, rfc3920bis-17]  | 5.7.3.7.8.2   | R                           |
| 12 | Client and server implementations SHALL qualify the root <stream/> element ("stream header") by the namespace "http://etherx.jabber.org/streams" (the "streams namespace"). If this rule is violated, the entity that receives the offending stream header SHALL return a stream error to the sending entity, which SHALL be either <invalid-namespace/> or <bad-format/>. [Section 4.7.1, rfc3920bis-17]   | 5.7.3.7.9.1   | R                           |
| 13 | An entity (client or server) SHALL declare a content namespace for data sent over the stream. The content namespace SHALL be the same for the initial stream and the response stream so that both streams are qualified consistently. The content namespace applies to all first-level child elements sent over the stream unless explicitly qualified by another namespace. [Section 4.7.2, rfc3920bis-17]   | 5.7.3.7.9.2   | R                           |
|    | The XMPP defines two content namespaces: "jabber:client" and "jabber:server." Client implementations SHALL support the jabber:client content namespace. Server implementations SHALL support both the jabber:client content namespace (when the stream is used for communication between a client and a server) and the jabber:server content namespace (when the stream is used for communication between two servers). [Section 4.7.5, rfc3920bis-17] |               |                             |
|    | If an entity receives a first-level child element qualified by a content namespace it does not support, it SHALL return an <invalid-namespace/> stream error. [Section 4.7.5, rfc3920bis-17]  |               |                             |
| 14 | The error child SHALL be sent by an entity (client or server) if it perceives that a stream-level error has occurred. [Section 4.8, rfc3920bis-17]  | 5.7.3.7.10    | R                           |
|    | Stream-level errors are unrecoverable. Therefore, if an error occurs at the level of the stream, the entity (client or server) that detects the error SHALL send an <error/> element with an appropriate child element that specifies the error condition and at the same time send a closing </stream> tag. [Section 4.8.1.1, rfc3920bis-17]   |               |                             |
|    | The entity that generates the stream error then SHALL close the stream as explained under Section 4.4 of rfc3920bis-17. [Section 4.8.1.1, rfc3920bis-17]  |               |                             |
|    | If the error is triggered by the initial stream header, the receiving entity SHALL still send the opening <stream> tag, include the <error/> element as a child of the stream element, and then send the closing </stream> tag (preferably all at the same time). [Section 4.8.1.2, rfc3920bis-17]  |               |                             |
| 15 | All XML streams (i.e., including both client-to-server and server-to-server connections) SHALL be secured with the use of the TLS protocol.   | 5.7.3.8       | R                           |
| 16 | This specification mandates the use of the STARTTLS command to initiate TLS negotiation. All client and server implementations SHALL support and use the "STARTTLS" extension.  | 5.7.3.8.1     | R                           |
|    | Immediately after the opening of the response stream, the receiving entity SHALL initiate the process of stream negotiation. [Section 5.4.1, rfc3920bis-17]   |               |                             |
|    | In the stream feature announcement provided by the receiving entity during the initial stage of the stream negotiation process, the receiving entity SHALL advertize ONLY the STARTTLS feature (qualified by the XML namespace: "urn:ietf:params:xml:ns:xmpp-tls") and SHALL also include an empty <required/> child element. [Section 5.4.1, rfc3920bis-17]  |               |                             |
| 17 | In order to begin the STARTTLS negotiation, the initiating entity SHALL issue the STARTTLS command (i.e., a <starttls/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace) to instruct the receiving entity that it wishes to begin a STARTTLS negotiation to secure the stream. [Section 5.4.2.1, rfc3920bis-17]  | 5.7.3.8.2     | R                           |
|    | The receiving entity SHALL reply with a <proceed/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace. [Section 5.4.2.1, rfc3920bis-17]   |               |                             |
| 18 | If there is a failure of STARTTLS negotiations, the receiving entity SHALL return a <failure/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace and SHALL close the XML stream. [Section 5.4.2.2, rfc3920bis-17]  | 5.7.3.8.3     | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 19 | After the receiving entity has sent and the initiating entity has received the <proceed/> element, the initiating and receiving entities SHALL proceed to TLS negotiation. The TLS negotiation and implementation SHALL be in accordance with the requirements defined in UCR Section 5.4, Information Assurance Requirements. Section 5.4 provides detailed guidance and requirements regarding the use of TLS with DoD PKI certificates.  | 5.7.3.8.4     | R                           |
| 20 | If the TLS negotiation is successful, then the initiating and receiving entities SHALL proceed. [Section 5.4.3.3, rfc3920bis-17]  | 5.7.3.8.5     | R                           |
| 21 | If the TLS negotiation results in failure, the receiving entity SHALL terminate the TCP connection. [Section 5.4.3.2, rfc3920bis-17]  | 5.7.3.8.6     | R                           |
| 22 | Client and server implementations SHALL complete STARTTLS negotiation before proceeding to SASL protocol negotiation; this order of negotiation is necessary to help safeguard authentication information sent during SASL negotiation, as well as to make it possible to base the use of the SASL EXTERNAL mechanism on a certificate provided during prior TLS negotiation (for entities who authenticate using a DoD PKI certificate). [Section 5.3.4, rfc3920bis-17]  | 5.7.3.8.7     | R                           |
| 23 | If the STARTTLS negotiation fails, the receiving entity SHALL return a <failure/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace, terminate the XML stream, and terminate the underlying TCP connection. [Section 5.4.2.2, rfc3920bis-17]   | 5.7.3.8.8     | R                           |
| 24 | The XMPP includes a method for adding authentication support to an XML stream by means of an XMPP-specific profile of the SASL protocol. As described in RFC 4422, SASL is a framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms. [Section 6 of rfc3920bis-17 and RFC 4422]   | 5.7.3.9       | R                           |
|    | All client and server implementations SHALL support SASL negotiations. [Section 6.2, rfc3920bis-17]   |               |                             |
|    | The entities involved in an XML stream SHALL consider SASL as mandatory-to-negotiate. [Section 6.3.1, rfc3920bis-17]  |               |                             |
|    | Anonymous login capability is prohibited. [Instant Messaging STIG, Version 1, Release 2]  |               |                             |
| 25 | During the prior TLS negotiation, the server SHALL authenticate using a DoD PKI certificate. The client SHALL validate the certificate presented by the server (i.e., shall verify that the certificate is unexpired, unrevoked, and anchored to a trusted DoD CA in accordance with the policies and requirements defined in UCR Section 5.4).   | 5.7.3.9.1     | R                           |
|    | The client SHALL authenticate using name and password using the SASL PLAIN mechanism.   |               |                             |
|    | After successful STARTTLS negotiation, the server SHALL offer the SASL PLAIN mechanism to the client during SASL negotiation. The <mechanisms/> element SHALL be qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace. The <mechanisms/> element SHALL contain one <mechanism/> child element including the appropriate value for the PLAIN mechanism. [Section 6.4.1, rfc3920bis-17]  |               |                             |
|    | The client SHALL select the PLAIN authentication mechanism by sending an <auth/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace and which SHALL include the appropriate value for the PLAIN 'mechanism' attribute.   |               |                             |
|    | Upon receipt of the message, the server will verify the presented authentication identity and password by performing a directory lookup to a directory service linked to the XMPP server for authenticating the user. [Instant Messaging STIG, Version 1, Release 2]  |               |                             |
|    | All users SHALL be linked to a directory service, which is linked to the user's home XMPP server. [Instant Messaging STIG, Version 1, Release 2]  |               |                             |
|    | The server SHALL report the success of the handshake by sending a <success/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace [Section 6.4.6, rfc3920bis-17]   |               |                             |
|    | After successful SASL negotiation, the client and server SHALL restart the stream. Upon receiving the <success/> element, the client SHALL initiate a new stream over the existing TLS connection by sending a new initial stream header to the server. The client SHALL NOT send a closing </stream> tag before sending the new initial stream header, since the server and client MUST consider the original stream to be replaced upon sending or receiving the <success/> element. [Section 6.4.6, rfc3920bis-17] |               |                             |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 25 | Upon receiving the new initial stream header from the client, the server SHALL respond by sending a new response stream header to the client (for which it SHALL generate a new stream ID instead of re-using the old stream ID). [Section 6.4.6, rfc3920bis-17]  | 5.7.3.9.1     | R                           |
|    | The server SHALL also send stream features, containing any further available features or containing no features (via an empty <features/> element). [Section 6.4.6, rfc3920bis-17]  |               |                             |
| 26 | During the prior TLS negotiation, the initiating entity and the receiving entity SHALL mutually authenticate using DoD PKI certificates.  | 5.7.3.9.2     | R                           |
|    | After the successful mutual authentication of the receiving entity and the initiating entity during the prior TLS negotiation, the receiving entity SHALL offer the SASL EXTERNAL mechanism (as defined in Appendix A of RFC 4422) to the initiating entity during SASL negotiation. [Section 6.3.4, rfc3920bis-17]   |               |                             |
|    | In response to the receiving entity offering the SASL EXTERNAL mechanism, the initiating entity SHALL select the EXTERNAL authentication mechanism by sending an <auth/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace and which SHALL include the appropriate value for the EXTERNAL 'mechanism' attribute and which also includes an empty response of "=". [Section 6.4, rfc3920bis-17 and Section 3, XEP-178]   |               |                             |
|    | The receiving entity SHALL report the success of the handshake by sending a <success/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace [Section 6.4.6, rfc3920bis-17]   |               |                             |
|    | After successful SASL negotiation, the initiating entity and the receiving entity SHALL restart the stream. Upon receiving the <success/> element, the initiating entity SHALL initiate a new stream over the existing TLS connection by sending a new initial stream header to the receiving entity. The initiating entity SHALL NOT send a closing </stream> tag before sending the new initial stream header, since the receiving entity and initiating entity MUST consider the original stream to be replaced upon sending or receiving the <success/> element. [Section 6.4.6, rfc3920bis-17] |               |                             |
|    | Upon receiving the new initial stream header from the initiating entity, the receiving entity SHALL respond by sending a new response stream header to the initiating entity (for which it SHALL generate a new stream ID instead of reusing the old stream ID). [Section 6.3.2, and Section 6.4.6, rfc3920bis-17]  |               |                             |
| 27 | The receiving entity SHALL also send stream features, containing any further available features or containing no features (via an empty <features/> element). [Section 6.4.6, rfc3920bis-17]  | 5.7.3.9.3     | R                           |
|    | The receiving entity SHALL report failure of the handshake by sending a <failure/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace. [Section 6.4.5, rfc3920bis-17]  |               |                             |
|    | The particular cause of failure SHALL be communicated in an appropriate child element of the <failure/> element as defined under Section 6.4 (SASL Errors) of rfc3920bis-17. [Section 6.4.5, rfc3920bis-17]   |               |                             |
|    | The receiving entity SHALL allow a configurable number of retries (at least two and no more than three per IM STIG policy).<br>If the initiating entity exceeds the maximum number of retries, the server SHALL return a stream error (which SHALL be either <policy-violation/> or <not-authorized/>). [Section 6.4.5, rfc3920bis-17]  |               |                             |
| 28 | All client and server implementations SHALL support resource binding. [Section 7.2, rfc3920bis-17]  | 5.7.3.10.2.1  | R                           |
|    | For client-to-server connections, both the client and server SHALL consider resource binding as mandatory-to-negotiate. [Section 7.3.1, rfc3920bis-17]  |               |                             |
| 29 | Upon sending a new response stream header to the client after successful SASL negotiation, the server SHALL include a <bind/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-bind' namespace in the stream features it presents to the client. [Section 7.4, rfc3920bis-17]  | 5.7.3.10.2.2  | R                           |
| 30 | A server implementation SHALL be able to generate an XMPP resourcepart on behalf of a client. [Section 7.6, rfc3920bis-17]  | 5.7.3.10.2.3  | R                           |
|    | A resourcepart SHALL at a minimum be unique among the connected resources for a specific local account in the form of <localpart@domain>. Enforcement of this policy is the responsibility of the server.   |               |                             |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 30 | A client SHALL request a server-generated resourcepart by sending an Info/Query (IQ) stanza of type "set" (see UCR Section 5.7.3.12.2, Roster-Related Methods) containing an empty <bind/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-bind' namespace. [Section 7.6.1, rfc3920bis-17]   | 5.7.3.10.2.3  | R                           |
|    | Once the server has generated an XMPP resourcepart for the client, it SHALL return an IQ stanza of type "result" to the client, which SHALL include a <jid/> child element that specifies the full JID for the connected resource as determined by the server. [Section 7.6.1, rfc3920bis-17]  |               |                             |
| 31 | Client and server implementations SHALL support the syntax and semantics associated with the message, presence, and IQ stanzas. [See the following UCR sections 5.7.3.11.1 through 5.7.3.11.3]   | 5.7.3.11      | R                           |
| 32 | <p>The following rules SHALL be followed regarding the use of the 'to' attribute in the context of XML streams qualified by the 'jabber:client' namespace (i.e., client-to-server streams) [Section 8.1.1.1, rfc3920bis-17]</p> <p>a. A stanza with a specific intended recipient SHALL possess a 'to' attribute whose value is an XMPP address.</p> <p>b. A stanza sent from a client to a server for direct processing by the server on behalf of the client (e.g., presence sent to the server for broadcasting to other entities) SHALL NOT possess a 'to' attribute.</p>  | 5.7.3.11.1.1  | R                           |
|    | <p>The following rules SHALL be followed regarding the use of the 'to' attribute in the context of XML streams qualified by the 'jabber:server' namespace (i.e., server-to-server streams) [Section 8.1.1.2, rfc3920bis-17]:</p> <p>a. A stanza SHALL possess a 'to' attribute whose value is an XMPP address; if a server receives a stanza that does not meet this restriction, it SHALL generate an &lt;improperaddressing/&gt; stream error.</p> <p>b. The domain identifier portion of the JID in the 'to' attribute SHALL match a hostname serviced by the receiving server; if a server receives a stanza that does not meet this restriction, it SHALL generate a &lt;host-unknown/&gt; or &lt;host-gone/&gt; stream error.</p>  |               |                             |
| 33 | <p>The following rules SHALL be followed regarding the use of the 'from' attribute in the context of XML streams qualified by the 'jabber:client' namespace (i.e., client-to-server streams) [Section 8.1.2.1, rfc3920bis-17]:</p> <p>a. When the server receives an XML stanza from a client, the server SHALL add a 'from' attribute to the stanza or override the 'from' attribute specified by the client, where the value of the 'from' attribute is the full JID (&lt;localpart@domainpart/resource&gt;) determined by the server for the connected resource that generated the stanza or the bare JID (&lt;localpart@domainpart&gt;) in the case of subscription-related presence stanzas.</p> <p>b. When the server generates a stanza from the server itself for delivery to the client, the stanza SHALL include a 'from' attribute whose value is the bare JID (i.e., &lt;domain&gt;) of the server as agreed upon during stream negotiation (e.g., based on the 'to' attribute of the initial stream header).</p> <p>c. When the server generates a stanza from the server for delivery to the client on behalf of the account of the connected client (e.g., in the context of data storage services provided by the server on behalf of the client), the stanza SHALL either (a) not include a 'from' attribute or (b) include a 'from' attribute whose value is the account's bare JID (&lt;localpart@domainpart&gt;).</p> <p>d. A server SHALL NOT send to the client a stanza without a 'from' attribute if the stanza was not generated by the server (e.g., if it was generated by another client or another server).</p> <p>e. When a client receives a stanza that does not include a 'from' attribute, it SHALL assume that the stanza is from the user's account on the server.</p> | 5.7.3.11.1.2  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 33 | <p>The following rules SHALL be followed regarding the use of the 'from' attribute in the context of XML streams qualified by the 'jabber:server' namespace (i.e., server-to-server streams) [Section 8.1.2.2, rfc3920bis-17]:</p> <p>a. A stanza SHALL possess a 'from' attribute whose value is an XMPP address; if a server receives a stanza that does not meet this restriction, it SHALL generate an &lt;improper-addressing/&gt; stream error.</p> <p>b. The domain identifier portion of the JID contained in the 'from' attribute SHALL match the hostname of the sending server (or any validated domain thereof) as communicated in the SASL negotiation; if a server receives a stanza that does not meet this restriction, it SHALL generate an &lt;invalid-from/&gt; stream error.</p> <p>Enforcement of these rules helps to prevent certain denial of service attacks.</p> | 5.7.3.11.1.2  | R                           |
| 34 | <p>For &lt;iq/&gt; stanzas, the originating entity SHALL include an 'id' attribute. [Section 8.1.3, rfc3920bis-17]</p> <p>NOTE: For &lt;message/&gt; and &lt;presence/&gt; stanzas, it is recommended for the originating entity to include an 'id' attribute. [Section 8.1.3, rfc3920bis-17]</p> <p>If the generated stanza includes an 'id' attribute, then it is required for the associated response or error stanza to also include an 'id' attribute, where the value of the 'id' attribute SHALL match that of the generated stanza. [Section 8.1.3, rfc3920bis-17]</p>   | 5.7.3.11.1.3  | R                           |
| 35 | <p>As discussed in Section 8.1.4 of rfc3920bis-17, the 'type' attribute specifies the purpose or context of the message, presence, or IQ stanza. The particular allowable values for the 'type' attribute vary depending on whether the stanza is a message, presence, or IQ stanza. The defined values for message and presence stanzas are specific to instant messaging and presence applications and therefore are defined in subsequent sections of this specification (e.g., 5.7.3.13, 5.7.3.14, 5.7.3.15, 5.7.3.17), whereas the values for IQ stanzas specify the role of an IQ stanza in a structured request-response exchange and therefore are specified under UCR Section 5.7.3.11.2.3, IQ Semantics. The only 'type' value common to all three stanzas is "error"; see UCR Section 5.7.3.11.3, Stanza Errors. [Section 8.1.4, rfc3920bis-17]</p>                             | 5.7.3.11.1.4  | R                           |
| 36 | <p>If an inbound stanza received by a client or server does not possess an 'xml:lang' attribute, an implementation SHALL assume that the default language is that which is specified for the stream. [Section 8.1.5, rfc3920bis-17]</p> <p>A server SHALL NOT modify or delete the 'xml:lang' attribute of stanzas it receives from other entities. [Section 8.1.5, rfc3920bis-17]</p>   | 5.7.3.11.1.5  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference  | Required (R) Conditions (C) |
|----|---|----------------|-----------------------------|
| 37 | <p>When a client or server implementation generates or processes an IQ stanza, the following rules apply [Section 8.2.3, rfc3920bis-17]:</p> <p>a. An IQ stanza SHALL include the 'id' attribute.</p> <p>b. An IQ stanza SHALL include the 'type' attribute.</p> <p>c. The value of the 'type' attribute for IQ stanzas SHALL be one of the following (if the value is other than one of the following strings, the recipient or an intermediate server SHALL return a stanza error of &lt;bad-request/&gt;):</p> <p>(1) get – The stanza requests information (i.e., the stanza inquires about data which is needed in order to complete further operations, etc)</p> <p>(2) set – The stanza provides data that is needed for an operation to be completed (e.g., it sets new values, replaces existing values, etc)</p> <p>(3) result – The stanza is a response to a successful “get” or “set” request</p> <p>(4) error – The stanza reports an error that has occurred regarding the processing or delivery of a previously sent “get” or “set” request</p> <p>d. An entity that receives an IQ request of type “get” or “set” SHALL reply with an IQ response of type “result” or “error”. The response SHALL preserve the 'id' attribute of the request.</p> <p>e. An entity that receives a stanza of type “result” or “error” SHALL NOT respond to the stanza by sending a further IQ response of type “result” or “error”.</p> <p>f. An IQ stanza of type “get” or “set” SHALL contain exactly one child element, which specifies the semantics of the particular request.</p> <p>g. An IQ stanza of type “result” SHALL include zero or one child element.</p> <p>h. An IQ stanza of type “error” SHALL include an &lt;error/&gt; child.</p> | 5.7.3.11.2.3   | R                           |
| 38 | Client and server implementations SHALL comply with the mandatory requirements defined in Section 8.3 of rfc3920bis-17.   | 5.7.3.11.3     | R                           |
| 39 | <p>If the domainpart of the JID contained in the 'to' attribute does not match one of the configured hostnames of the server itself, the server SHALL attempt to route the stanza to the remote domain. [Section 10.4, rfc3920bis-17]</p> <p>NOTE: These rules apply only to client-to-server streams. As described under UCR Section 5.7.3.11.1.1, Server-to-Server Streams, a server SHALL NOT accept a stanza over a server-to-server stream if the domainpart of the JID in the 'to' attribute does not match a hostname serviced by the receiving server. [Section 10.4, rfc3920bis-17]</p>  | 5.7.3.11.4.1   | R                           |
| 40 | If a server-to-server stream already exists between the two domains, the sender's server SHALL attempt to route the stanza to the authoritative server for the remote domain over the existing stream. [Section 10.4.1, rfc3920bis-17]  | 5.7.3.11.4.1.1 | R                           |
| 41 | <p>If no server-to-server stream exists between the two domains, the sender's server SHALL proceed as follows [Section 10.4.2, rfc3920bis-17]:</p> <ul style="list-style-type: none"> <li>□ Resolve the hostname of the remote domain, as described in UCR Section 5.7.3.7.1.1.</li> <li>□ Negotiate a server-to-server stream between the two domains (as defined in Section 5.7.3.8, TLS and STARTTLS Negotiation, and CR Section 5.7.3.9, Authentication and SASL Negotiation.</li> <li>□ Route the stanza to the authoritative server for the remote domain over the newly-established stream.</li> </ul>   | 5.7.3.11.4.1.2 | R                           |
| 42 | If the routing of a stanza to the intended recipient's server is unsuccessful, the sender's server SHALL return an error to the sender. If resolution of the remote domain is unsuccessful, the stanza error SHALL be <remote-server-not-found/>. If the resolution succeeds, but the XML streams cannot be negotiated, the stanza error SHALL be <remote-server-timeout/>. [Section 10.4.3, rfc3920bis-17]   | 5.7.3.11.4.1.3 | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference  | Required (R) Conditions (C) |
|----|---|----------------|-----------------------------|
| 42 | If stream negotiation with the intended recipient's server is successful but the remote server cannot deliver the stanza to the recipient, the remote server SHALL return an appropriate error to the sender by way of the sender's server. [Section 10.4.3, rfc3920bis-17]   | 5.7.3.11.4.1.3 | R                           |
| 43 | If the hostname of the domainpart of the JID contained in the 'to' attribute matches one of the configured hostnames of the server, the server SHALL first determine if the hostname is serviced by the server itself or by a specialized local service. If the latter, the server SHALL route the stanza to that service. If the former, the server SHALL proceed as follows [Section 10.5.3, rfc3920bis-17]   | 5.7.3.11.4. 2  | R                           |
| 44 | <p>If there is no local account associated with the &lt;localpart@domainpart&gt;, how the stanza is processed depends on the stanza type. [Section 10.5.3.1, rfc3920bis-17]</p> <p>□□ For a message stanza, the server SHALL return a &lt;service-unavailable/&gt; stanza error to the sender.</p> <p>□□ For a presence stanza, the server SHALL ignore the stanza.</p> <p>□□ For an IQ stanza, the server SHALL return a &lt;service-unavailable/&gt; stanza error to the sender.</p>  | 5.7.3.11.4.2.1 | R                           |
| 45 | <p>If the JID contained in the 'to' attribute is of the form &lt;localpart@domainpart&gt;, how the stanza is processed depends on the stanza type. [Section 10.5.3.2, rfc3920bis-17]</p> <p>□ For a message stanza, if at least one connected resource for the account exists, the server SHALL deliver it to at least one of the connected resources. If there exists no connected resource, the server SHALL either return a &lt;service-unavailable/&gt; stanza error or store the message offline for delivery when the account next has a connected resource.</p> <p>□ For a presence stanza, if at least one connected resource that has sent initial presence exists (i.e., has a "presence session"), the server SHALL deliver it to such resources. If no connected resource exists, the server SHALL ignore the stanza.</p> <p>□ For an IQ stanza, the server SHALL handle it directly on behalf of the intended recipient.</p>   | 5.7.3.11.4.2.2 | R                           |
| 46 | <p>If the JID contained in the 'to' attribute is of the form &lt;localpart@domainpart/resource&gt; and there is no connected resource that exactly matches the full JID, the stanza SHALL be processed as if the JID were of the form &lt;localpart@domainpart&gt;. [Section 10.5.3.3, rfc3920bis-17]</p> <p>If the JID contained in the 'to' attribute is of the form &lt;localpart@domainpart/resource&gt; and there is a connected resource that exactly matches the full JID, the server SHALL deliver the stanza to that connected resource. [Section 10.5.3.3, rfc3920bis-17]</p>   | 5.7.3.11.4.2.3 | R                           |
| 47 | <p>Client and server implementations SHALL use IQ stanzas containing a &lt;query/&gt; child element qualified by the 'jabber:iq:roster' namespace to manage elements in a roster. [Section 2.1, rfc3921bis-15]</p> <p>Client and server implementations SHALL support the 'subscription' attribute and the allowable subscription-related values for this attribute. The state of the presence subscription in relation to a roster item is captured in the 'subscription' attribute of the &lt;item/&gt; element. The allowable subscription-related values for this attribute are [Section 2.1.2.5, rfc3921bis-15]:</p> <p>a. "none" – the user does not have a subscription to the contact's presence, and the contact does not have a subscription to the user's presence; this is the default value, so if the subscription attribute is not included, then the state is to be understood as "none"</p> <p>b. "to" – the user has a subscription to the contact's presence, but the contact does not have a subscription to the user's presence</p> <p>c. "from" – the contact has a subscription to the user's presence, but the user does not have a subscription to the contact's presence</p> <p>d. "both" – both the user and the contact have subscriptions to each other's presence (also called a "mutual subscription")</p> | 5.7.3.12.1     | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 47 | In a roster result, the client SHALL ignore values of the 'subscription' attribute other than "none", "to", "from", or "both". [Section 2.1.2.5, rfc3921bis-15]  | 5.7.3.12.1    | R                           |
|    | In a roster push, the client SHALL ignore values of the 'subscription' attribute other than "none", "to", "from", "both", or "remove". [Section 2.1.2.5, rfc3921bis-15]  |               |                             |
|    | In a roster set, the value of the 'subscription' can have a value of "remove", which indicates that the item is to be removed from the roster; the server SHALL ignore all values of the 'subscription' attribute other than "remove". [Section 2.1.2.5, rfc3921bis-15]  |               |                             |
|    | Client implementations SHALL support the 'name' attribute, which is used to specify the "handle" to be associated with the JID, as determined by the user (not the contact). It is optional for a client to include the 'name' attribute when adding or updating a roster item. [Section 2.1.2.4, rfc3921bis-15]   |               |                             |
|    | Client and server implementations SHALL support the 'ask' attribute, which is used to specify presence subscriptions sub-state. [Section 2.1.2.2, rfc3921bis-15]   |               |                             |
|    | A value of "subscribe" in the 'ask' attribute is used to signal a "Pending Out" sub-state as described under Section 3.1.2 of rfc3921bis-15. A server SHALL include the 'ask' attribute to inform the client of "Pending Out" sub-state. [Section 2.1.2.2, rfc3921bis-15]  |               |                             |
|    | <p>Client and server implementations SHALL support the &lt;group/&gt; child element which is used to specify a category or "bucket" into which the roster item is to be grouped by a client. It is optional for a client to include the &lt;group/&gt; element when adding or updating a roster item. If a roster set (Roster Set) includes no &lt;group/&gt; element, then the item is to be interpreted as being affiliated with no group. [Section 2.1.2.6, rfc3921bis-15]</p> <p>NOTE: An &lt;item/&gt; element MAY contain more than one &lt;group/&gt; element, which means that roster groups are not exclusive. [Section 2.1.2.6, rfc3921bis-15]</p> |               |                             |
| 48 | A client implementation SHALL have the ability to generate a Roster Get. A Roster Get is a client's request for the server to return the roster; syntactically it is an IQ stanza of type "get" sent from client to server and containing a <query/> element qualified by the 'jabber:iq:roster' namespace, where the <query/> element SHALL NOT contain any <item/> child elements. Likewise, a compliant server implementation SHALL be able to process this request. The expected outcome of sending a roster get is for the server to return a roster result. [Section 2.1.3, rfc3921bis-15]   | 5.7.3.12.2    | R                           |
|    | A server implementation SHALL be able to process a Roster Get.   |               |                             |
|    | A server implementation SHALL have the ability to generate a Roster Result. A Roster Result is the server's response to a roster get; syntactically it is an IQ stanza of type "result" sent from server to client and containing a <query/> element qualified by the 'jabber:iq:roster' namespace. The <query/> element in a roster result contains one <item/> element for each contact and therefore can contain more than one <item/> element. The ability to generate this response is required for server implementations. Likewise, a compliant client implementation SHALL be able to process this response. [Section 2.1.4, rfc3921bis-15]          |               |                             |
|    | A client implementation SHALL be able to process a Roster Result.  |               |                             |
|    | A client implementation SHALL have the ability to generate a Roster Set. A Roster Set is a client's request for the server to modify (i.e., create, update, or delete) a roster item; syntactically it is an IQ stanza of type "set" sent from client to server and containing a <query/> element qualified by the 'jabber:iq:roster' namespace. [Section 2.1.5, rfc3921bis-15]  |               |                             |
|    | A server implementation SHALL be able to process a Roster Set.   |               |                             |
|    | A server implementation SHALL have the ability to generate a Roster Push. A Roster Push is a newly created, updated, or deleted roster item that is sent from the server to the client; syntactically it is an IQ stanza of type "set" sent from server to client and containing a <query/> element qualified by the 'jabber:iq:roster' namespace. [Section 2.1.6, rfc3921bis-15]  |               |                             |
|    | A client implementation SHALL be able to process a Roster Push.  |               |                             |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 48 | As mandated by the semantics of the IQ stanza as defined in [rfc3920bis-17] each resource that receives a roster push SHALL reply with an IQ stanza of type 'result' (or 'error').<br><br>C: <iq from='john@example1.dod.mil/desktop client' id='a78b4q6ha463' type='result'/>   | 5.7.3.12.2    | R                           |
| 49 | Upon authenticating with a server and binding a resource (thus becoming a connected resource), a client SHALL request the roster before sending initial presence. A client requests the roster by sending a roster get over its stream to the server. [Section 2.2, rfc3921bis-15]<br><br>The server SHALL process the roster get and SHALL return a roster result containing a <query/> element qualified by the 'jabber:iq:roster' namespace. The <query/> element in a roster result SHALL contain one <item/> element for each contact and therefore can contain more than one <item/> element. [Section 2.1.3 and Section 2.2, rfc3921bis-15]<br><br>If the server cannot process the roster get, it SHALL return an appropriate stanza error as described in rfc3920bis-17.  | 5.7.3.12.3    | R                           |
| 50 | A client SHALL support the ability to add an item to the roster by sending a roster set containing a new item. [Section 2.3.1, rfc3921bis-15]<br><br>If the server can successfully process the roster set for the new item (i.e., if no error occurs), it SHALL create the roster item in persistent storage. The server SHALL then return an IQ stanza of type "result" to the connected resource that sent the roster set. [Section 2.3.2, rfc3921bis-15]<br><br>The server SHALL also send a roster push containing the new roster item to all of the user's interested resources, including the resource that generated the roster set. [Section 2.3.2, rfc3921bis-15]<br><br>If the server cannot successfully process the roster set, it SHALL return a stanza error. For additional details, see Section 2.3.3 of rfc3921bis-15.   | 5.7.3.12.4    | R                           |
| 51 | A client SHALL support the ability to update a roster item by sending a roster set to the server. Because a roster item is atomic, the item SHALL be updated exactly as provided in the roster set. [Section 2.4.1, rfc3921bis-15]<br><br>As with adding a roster item, if the roster item can be successfully processed, then the server SHALL update the roster information in persistent storage, send a roster push to the entire user's interested resources, and send an IQ result to the initiating resource. [Section 2.4.2, rfc3921bis-15]  | 5.7.3.12.5    | R                           |
| 52 | A client SHALL support the ability to delete a roster item by sending a roster set and specifying the value of the 'subscription' attribute to "remove". [Section 2.5.1, rfc3921bis-15]<br><br>As with adding a roster item, if the server can successfully process the roster set then it SHALL update the roster information in persistent storage, send a roster push to all of the user's interested resources (with the 'subscription' attribute set to a value of 'remove'), and send an IQ result to the initiating resource. [Section 2.5.2, rfc3921bis-15]<br><br>The user's server SHALL generate one or more subscription-related presence stanzas, as per the following use cases [Section 2.5.2, rfc3921bis-15]:<br><br>a. If the user has a presence subscription to the contact, then the user's server SHALL send a presence stanza of type "unsubscribe" to the contact (to unsubscribe from the contact's presence).<br><br>b. If the contact has a presence subscription to the user, then the user's server SHALL send a presence stanza of type "unsubscribed" to the contact (to cancel the contact's subscription to the user), or both.<br><br>c. If the presence subscription is mutual, then the user's server SHALL send both a presence stanza of type "unsubscribe" and a presence stanza of type "unsubscribed" to the contact.<br><br>S: <presence from='john@example1.dod.mil' id='lm3ba81g' to='robert@example2.dod.mil' type='unsubscribe'/> | 5.7.3.12.6    | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 52 | If the value of the 'jid' attribute specifies an item that is not in the roster, then the server SHALL return an <item-not-found/> stanza error. [Section 2.5.3, rfc3921bis-15]  | 5.7.3.12.6    | R                           |
| 53 | <p>A client implementation SHALL be capable of generating a subscription request by sending a presence stanza of type "subscribe". [Section 3.1.1, rfc3921bis-15]</p> <p>UC: &lt;presence id='xk3h1v69' to='john@example1.dod.mil' type='subscribe'/&gt;</p> <p>When the client sends a presence subscription request to a potential instant messaging and presence contact, the value of the 'to' attribute SHALL be a bare JID &lt;contact@domain&gt; rather a full JID &lt;contact@domain/resource&gt;. [Section 3.1.1, rfc3921bis-15]</p>  | 5.7.3.13.1.1  | R                           |
| 54 | <p>Upon receiving the outbound presence subscription request, the user's server SHALL comply with the following rules for Server Processing of Outbound Subscription Requests as defined below [Section 3.1.2, rfc3921bis-15]:</p> <p>a. Before processing the request, the user's server SHALL check the syntax of the JID contained in the 'to' attribute. If the JID is of the form &lt;localpart@domain/resourcepart&gt; instead of &lt;localpart@domain&gt;, the user's server SHALL treat it as if the request had been directed to the contact's bare JID and modify the 'to' address accordingly.</p> <p>b. If the potential contact is hosted on the same server as the user, then the server SHALL adhere to the Rules for Server Processing of Inbound Subscription Requests (see below) and SHALL deliver it to the local contact.</p> <p>c. If the potential contact is hosted on a remote server, the user's server SHALL then route the stanza to that remote domain in accordance with the Server Rules for Processing XML Stanzas (e.g., see Section 5.7.3.11.4.1, Rules for Processing XML Stanzas to Remote Domains).</p> <p>When a server processes or generates an outbound presence stanza of type "subscribe", "subscribed", "unsubscribe", or "unsubscribed", the server SHALL stamp the outgoing presence stanza with the bare JID &lt;localpart@domain&gt; of the sending entity. Enforcement of this rule simplifies the presence subscription model and helps to prevent presence leaks. [Section 3.1.2, rfc3921bis-15]</p> <p>If the presence subscription request cannot be locally delivered or remotely routed (e.g., because the request is malformed, the local contact does not exist, the remote server does not exist, an attempt to contact the remote server times out, or any other error determined or experienced by the user's server), then the user's server SHALL return an appropriate error stanza to the user. [Section 3.1.2, rfc3921bis-15]</p> <p>After locally delivering or remotely routing the presence subscription request, the user's server SHALL then send a roster push to all of the user's interested resources, containing the potential contact with a subscription state of "none" and with notation that the subscription is pending (via an 'ask' attribute whose value is "subscribe"). [Section 3.1.2, rfc3921bis-15]:</p> <p>US: &lt;iq id='b89c5r7ib574' to='john.smith@chat.dod.mil/desktop client' type='set'&gt;<br/> &lt;query xmlns='jabber:iq:roster'&gt;<br/> &lt;item ask='subscribe'<br/> jid='„robert.jones@example2.dod.mil/desktop client“<br/> subscription='none'/&gt;<br/> &lt;/query&gt;<br/> &lt;/iq&gt;</p> | 5.7.3.13.1.2  | R                           |
| 55 | Before processing the inbound presence subscription request, the contact's server SHALL check the syntax of the JID contained in the 'to' attribute. If the JID is of the form <contact@domain/resource> instead of <contact@domain>, the contact's server SHALL treat it as if the request had been directed to the contact's bare JID and modify the 'to' address accordingly. [Section 3.1.3, rfc3921bis-15]  | 5.7.3.13.1.3  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 55 | <p>When processing the inbound presence subscription request, the user's server SHALL comply with the following rules for Server Processing of Inbound Subscription Requests as defined below [Section 3.1.3, rfc3921bis-15]:</p> <p>a. Above all, the contact's server SHALL NOT automatically approve subscription requests on the contact's behalf (unless the contact has configured its account to automatically approve subscription requests). Instead, the contact's server SHALL deliver that request to the contact's available resource(s) for approval or denial by the contact.</p> <p>b. If the contact exists and the user already has a subscription to the contact's presence, then the contact's server SHALL auto-reply on behalf of the contact by sending a presence stanza of type "subscribed" from the contact's bare JID to the user's bare JID.</p> <p>c. If the contact does not exist, then the contact's server SHALL automatically return a presence stanza of type "unsubscribed" to the user.</p> <p>d. Otherwise, if there is at least one available resource associated with the contact when the subscription request is received by the contact's server, then the contact's server SHALL broadcast that subscription request to all of the contact's available resources.</p> <p>e. Otherwise, if the contact exists, the user does not already have a subscription to the contact's presence, and the contact has no available resources when the subscription request is received by the contact's server, then the contact's server SHALL keep a record of the complete presence stanza comprising the subscription request, including any extended content contained therein, and deliver the request when the contact next has an available resource. The contact's server SHALL continue to deliver the subscription request whenever the contact creates an available resource, until the contact either approves or denies the request.</p> | 5.7.3.13.1.3  | R                           |
| 56 | <p>When the contact's client receives a subscription request from the user, it SHALL present the request to the contact for approval (unless the contact has explicitly configured the client to automatically approve or deny some or all subscription requests). [Section 3.1.4, rfc3921bis-15]</p> <p>A client implementation SHALL be capable of generating a subscription approval by sending a presence stanza of type "subscribed".</p> <p>CC: &lt;presence id='h4v1c4kj' to='robert@example2.dod.mil' type='subscribed'/&gt;</p> <p>A client implementation SHALL be capable of denying a subscription request by sending a presence stanza of type "unsubscribed". [Section 3.1.4, rfc3921bis-15]</p> <p>CC: &lt;presence id='h4v1c4kj' to='robert@example2.dod.mil' type='unsubscribed'/&gt;</p>   | 5.7.3.13.1.4  | R                           |
| 57 | <p>When the contact's client sends the subscription approval, the contact's server SHALL stamp the outbound stanza with the bare JID &lt;localpart@domain&gt; of the contact and locally deliver or remotely route the stanza to the user. [Section 3.1.5, rfc3921bis-15]</p> <p>CS: &lt;presence from='john@example1.dod.mil' id='h4v1c4kj' to='robert@example2.dod.mil' type='subscribed'/&gt;</p> <p>The contact's server then SHALL send an updated roster push to all of the contact's interested resources, with the 'subscription' attribute set to a value of "from". [Section 3.1.5, rfc3921bis-15]</p> <p>The contact's server SHALL then also send current presence to the user from each of the contact's available resources. [Section 3.1.5, rfc3921bis-15]</p>  | 5.7.3.13.1.5  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 58 | <p>When the user's server receives the subscription approval, it SHALL first check if the contact is in the user's roster with subscription='none' or subscription='from' and the 'ask' flag set to "subscribe" (see Appendix A of rfc3921bis-15). If this check is successful, then the user's server SHALL proceed as follows [Section 3.1.6, rfc3921bis-15]:</p>  | 5.7.3.13.1.6  | R                           |
|    | <p>a. Deliver the inbound subscription approval to all of the user's interested resources. This SHALL occur before sending the roster push described in the next step. [Section 3.1.6, rfc3921bis-15]<br/> US: &lt;presence from='john@example1.dod.mil' id='h4v1c4kj' to='robert@example2.dod.mil' type='subscribed'/&gt;</p>   |               |                             |
|    | <p>b. Initiate a roster push to all of the user's interested resources, containing an updated roster item for the contact with the 'subscription' attribute set to a value of "to" (if the subscription state was "None + Pending Out" or "None + Pending Out+In") or "both" (if the subscription state was "From + Pending Out"). See Table 5 of Appendix A of rfc3921bis-15. [Section 3.1.6, rfc3921bis-15]</p>  |               |                             |
|    | <p>US: &lt;iq id='b89c5r7ib576' to='robert@example2.dod.mil/desktop client' type='set'&gt;<br/> &lt;query xmlns='jabber:iq:roster'&gt;<br/> &lt;item jid='john@example1.dod.mil' subscription='to'/&gt;<br/> &lt;/query&gt;<br/> &lt;/iq&gt;</p> <p>c. The user's server SHALL also deliver the available presence stanza received from each of the contact's available resources to each of the user's available resources.</p>   |               |                             |
|    | <p>Otherwise – that is, if the user does not exist, if the contact is not in the user's roster, or if the contact is in the user's roster with a subscription state other than those described in the foregoing check – then the user's server SHALL silently ignore the subscription approval stanza by not delivering it to the user, not modifying the user's roster, and not generating a roster push to the user's interested resources. [Section 3.1.6, rfc3921bis-15]</p> |               |                             |
|    | <p>A client implementation SHALL be capable of sending a presence stanza of type "unsubscribed" in order to cancel a subscription that it has previously granted to a user. [Section 3.2.1, rfc3921bis-15]</p>   |               |                             |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 59 | <p>Upon receiving the outbound subscription cancellation, the contact's server SHALL proceed as follows [Section 3.2.2, rfc3921bis-15]:</p> <ol style="list-style-type: none"> <li>1. If the user is hosted on the same server as the contact, then the server SHALL adhere to the rules specified in the next section in processing the subscription cancellation.</li> <li>2. If the user is hosted on a remote server, the contact's server SHALL then route the stanza to that remote domain.</li> <li>3. As mentioned, before locally delivering or remotely routing the stanza, the contact's server SHALL stamp the outbound subscription cancellation with the bare JID &lt;localpart@domain&gt; of the contact.<br/>CS: &lt;presence from='john@example1.dod.mil' id='ij5b1v7g' to='robert@example2.dod.mil' type='unsubscribed'/&gt;</li> <li>4. The contact's server then SHALL send a roster push with the updated roster item to all of the contact's interested resources, where the subscription state is now either "none" or "to". For added clarification, see Appendix A of rfc3921bis-15.</li> <li>5. The contact's server then SHALL send a presence stanza of type "unavailable" from all of the contact's online resources to the user.<br/>CS: &lt;presence from='john@example1.dod.mil/desktop client' id='i8bsg3h3' type='unavailable'/&gt;</li> </ol>  | 5.7.3.13.2.2  | R                           |
| 60 | <p>When the user's server receives the inbound subscription cancellation, it SHALL first check if the contact is in the user's roster with subscription='to' or subscription='both' (see Appendix A of rfc3921bis-15).</p> <ol style="list-style-type: none"> <li>1. If this check is successful, the user's server SHALL [Section 3.2.3, rfc3921bis-15]: <ol style="list-style-type: none"> <li>a. Deliver the inbound subscription cancellation to all of the user's interested resources. This SHALL occur before sending the roster push described in the next step.<br/>US: &lt;presence from='john@example1.dod.mil' id='ij5b1v7g' to='robert@example2.dod.mil' type='unsubscribed'/&gt;</li> <li>b. Initiate a roster push to all of the user's interested resources, containing an updated roster item for the contact with the „subscription“ attribute set to a value of "none" (if the subscription state was "To" or "To + Pending In") or "from" (if the subscription state was "Both").</li> </ol> </li> <li>2. If the check (above) is not successful, that is, if the user does not exist, if the contact is not in the user's roster, or if the contact is in the user's roster with a subscription state other than those described in the foregoing check, then the user's server SHALL silently ignore the stanza by not delivering it to the user, not modifying the user's roster, and not generating a roster push to the user's interested resources. [Section 3.2.3, rfc3921bis-15]</li> </ol> | 5.7.3.13.2.3  | R                           |
| 61 | <p>To unsubscribe from a contact's presence, the client SHALL send a presence stanza of type "unsubscribe". [Section 3.3.1, rfc3921bis-15]</p> <p>UC: &lt;presence id='ul4bs71n' to='john@example.dod.mil' type='unsubscribe'/&gt;</p>  | 5.7.3.13.3.1  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 62 | <p>Upon receiving the outbound unsubscribe, the user's server SHALL proceed as follows [Section 3.3.2, rfc3921bis-15]:</p> <ol style="list-style-type: none"> <li>1. If the contact is hosted on the same server as the user, then the server SHALL adhere to the rules specified for Server Processing of Inbound Unsubscribe (see below).</li> <li>2. If the contact is hosted on a remote server, the user's server SHALL then route the stanza to that remote domain.</li> <li>3. The user's server then SHALL send a roster push with the updated roster item to all the user's interested resources, where the subscription state is now either "none" or "from" (see Appendix A of rfc3921bis-15).</li> </ol> <p>US: &lt;iq id='h37h3u1bv402'<br/>to='robert@example2.dod.mil/desktop client'<br/>type='set'<br/>&lt;query xmlns='jabber:iq:roster'<br/>&lt;item jid='john@example1.dod.mil'<br/>subscription='none'/&gt;<br/>&lt;/query&gt;<br/>&lt;/iq&gt;</p>  | 5.7.3.13.3.2  | R                           |
| 63 | <p>When the contact's server receives the unsubscribe notification, it SHALL first check if the user is in the contact's roster with subscription="from" or subscription="both" (i.e., a subscription state of "From", "From + Pending Out", or "Both"; see Appendix A of rfc3921bis-15).</p> <ol style="list-style-type: none"> <li>1. If this check is successful, the contact's server SHALL [Section 3.3.3, rfc3921bis-15]: <ol style="list-style-type: none"> <li>a. Deliver the inbound unsubscribe to all of the contact's interested resources. This SHALL occur before sending the roster push described in the next step.</li> <li>b. Initiate a roster push to all of the contact's interested resources, containing an updated roster item for the contact with the „subscription“ attribute set to a value of "none" (if the subscription state was "From" or "From + Pending Out") or "to" (if the subscription state was "Both").</li> <li>c. Generate an outbound presence stanza of type "unavailable" from each of the contact's available resources to the user.</li> </ol> </li> <li>2. If the check (above) is not successful, that is, if the contact does not exist, if the user is not in the contact's roster, or if the user is in the contact's roster with a subscription state other than those described in the foregoing check, then the contact's server SHALL silently ignore the stanza by not delivering it to the contact, not modifying the contact's roster, and not generating a roster push to the contact's interested resources. [Section 3.3.3, rfc3921bis-15]</li> </ol> | 5.7.3.13.3.3  | R                           |
| 64 | <p>After completing the mandatory-to-negotiate stream features and retrieving a roster, a client implementation SHALL signal its availability for communication by sending initial presence to its server, i.e., a presence stanza with no 'to' address and no 'type' attribute. [Section 4.2.1, rfc3921bis-15]</p> <p>UC: &lt;presence/&gt;</p> <p>NOTE: The initial presence stanza may contain the &lt;priority/&gt; element, the &lt;show/&gt; element, and one or more instances of the &lt;status/&gt; element. [Section 4.2, rfc3921bis-15]</p>   | 5.7.3.14.1.1  | R                           |
| 65 | <p>Upon receiving initial presence from a client, the user's server SHALL send the initial presence stanza from the full JID &lt;user@domain/resource&gt; of the user to all contacts that are subscribed to the user's presence. [Section 4.2.2, rfc3921bis-15]</p> <p>US: &lt;presence from='user@domain/resourcepart'<br/>to='contact@domain'/&gt;</p>  | 5.7.3.14.1.2  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 65 | The user's server SHALL also broadcast initial presence from the user's newly available resource to all of the user's available resources (including the resource that generated the presence notification in the first place). [Section 4.2.2, rfc3921bis-15]  | 5.7.3.14.1.2  | R                           |
|    | In the absence of presence information about the user's contacts, the user's server SHALL also send presence probes to the user's contacts on behalf of the user (see Section 5.7.3.14.2, Presence Probes). [Section 4.2.2, rfc3921bis-15]  |               |                             |
| 66 | Upon receiving presence from the user, the contact's server SHALL deliver the user's presence stanza to all of the contact's available resources. [Section 4.2.3, rfc3921bis-15]  | 5.7.3.14.1.3  | R                           |
| 67 | When the contact's client receives presence from the user, it SHALL proceed as follows [Section 4.2.4, rfc3921bis-15]:  | 5.7.3.14.1.4  | R                           |
|    | 1. If the user is in the contact's roster, the client SHALL display the presence information in an appropriate roster interface.<br><br>2. If the user is not in the contact's roster, the client SHALL ignore the presence information and not display it to the contact.  |               |                             |
| 68 | To discover the availability of a user's contact, the user's server SHALL be capable of sending a presence probe from the bare JID <user@domain> of the user to the bare JID <contact@domain> of the contact. [Section 4.3.1, rfc3921bis-15]<br><br>US: <presence from='john@example1.dod.mil' id='ign291v5' to='robert@example2.dod.mil' type='probe'/>  | 5.7.3.14.2.1  | R                           |
|    | The server SHALL NOT send a probe to a contact if the user is not subscribed to the contact's presence (i.e., if the contact is not in the user's roster with the „subscription“ attribute set to a value of “to” or “both”). [Section 4.3.1, rfc3921bis-15]<br><br>NOTE: The user's server SHOULD send a presence probe whenever the user starts a new presence session by sending initial presence. However, the server MAY choose not to send the probe at that point if it has what it deems to be reliable and up-to-date presence information about the user's contacts (e.g., because the user has another available resource or because the user briefly logged off and on before the new presence session began). In addition, a server MAY periodically send a presence probe to a contact if it has not received presence information or other traffic from the contact in some configurable amount of time; this can help to prevent “ghost” contacts who appear to be online but in fact are not. [Section 4.3.1, rfc3921bis-15]<br><br>NOTE: Naturally, the user's server does not need to send a presence probe to a contact if the contact's account resides on the same server as the user, since the server possesses the contact's information locally. [Section 4.3.1, rfc3921bis-15] |               |                             |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 69 | <p>Upon receiving a presence probe to the contact's bare JID from the user's server on behalf of the user, the contact's server SHALL reply as follows [Section 4.3.2, rfc3921bis-15]:</p> <ol style="list-style-type: none"> <li>1. If the contact account does not exist or the user is in the contact's roster with a subscription state other than "From", "From + Pending Out", or "Both" (as defined under Appendix A of rfc3921bis-15), then the contact's server SHALL return a presence stanza of type "unsubscribed" in response to the presence probe. Here the „from“ address SHALL be the bare JID of the contact, since specifying a full JID would constitute a presence leak as described in rfc3920bis-17.</li> </ol> <pre>CS: &lt;presence from='mike@example2.dod.mil' id='xv291f38' to='john@example1.dod.mil' type='unsubscribed'/&gt;</pre> <ol style="list-style-type: none"> <li>2. Else, if the contact has moved temporarily or permanently to another address, then the server SHALL return a presence stanza of type "error" with a stanza error condition of &lt;redirect/&gt; (temporary) or &lt;gone/&gt; (permanent) that includes the new address of the contact.</li> <li>3. Else, if the contact has no available resources, then the server SHALL reply to the presence probe by sending to the user a presence stanza of type "unavailable".</li> <li>4. Else, if the contact has at least one available resource, then the server SHALL reply to the presence probe by sending to the user the full XML of the last presence stanza with no „to“ attribute received by the server from each of the contact's available resources. Here the 'from' addresses are the full JIDs of each available resource.</li> </ol> <pre>CS: &lt;presence from='robert@example2.dod.mil/foo' id='hxf1v27k' to='john@example1.dod.mil'/&gt;</pre> | 5.7.3.14.2.2  | R                           |
| 70 | <p>After sending initial presence, a client implementation SHALL be capable of updating its availability by sending a presence stanza with no 'to' address and no 'type' attribute. [Section 4.4.1, rfc3921bis-15]</p> <pre>UC: &lt;presence&gt; &lt;show&gt;away&lt;/show&gt; &lt;/presence&gt;</pre> <p>NOTE: This presence update MAY contain the &lt;priority/&gt; element, the &lt;show/&gt; element, and one or more instances of the &lt;status/&gt; element.</p>  | 5.7.3.14.3    | R                           |
| 71 | <p>Upon receiving a presence stanza expressing updated availability, the user's server SHALL broadcast the full XML of that presence stanza to the contacts who meet all of the following criteria [Section 4.4.2, rfc3921bis-15]:</p> <ol style="list-style-type: none"> <li>a. The contact is in the user's roster with a subscription type of "from" or "both".</li> <li>b. The last presence stanza received from the contact during the user's presence session was NOT of type "unsubscribe".</li> </ol> <p>NOTE: As an optimization, if the subscription type is "both", then the server SHOULD send subsequent presence notifications to a contact only if the contact is online according to the user's server. [Section 4.4.2, rfc3921bis-15]</p> <p>The user's server SHALL also send the presence stanza to all of the user's available resources (including the resource that generated the presence notification in the first place). [Section 4.4.2, rfc3921bis-15]</p>  | 5.7.3.14.3.1  | R                           |
| 72 | <p>Upon receiving presence from the user, the contact's server SHALL deliver the user's presence stanza to all of the contact's available resources. [Section 4.4.3, rfc3921bis-15]</p>   | 5.7.3.14.3.2  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 73 | From the perspective of the contact's client, there is no significant difference between initial presence broadcast and subsequent presence broadcast, so the contact's client SHALL follow the rules for processing of inbound presence defined under Section 5.7.3.14.1.4, Client Processing of Inbound Initial Presence. [Section 4.4.4, rfc3921bis-15]  | 5.7.3.14.3.3  | R                           |
| 74 | <p>Before ending its presence session with a server, the user's client SHALL gracefully become unavailable by sending unavailable presence, i.e., a presence stanza that possesses no 'to' attribute and that possesses a 'type' attribute whose value is "unavailable". The unavailable presence stanza SHALL NOT contain the &lt;priority/&gt; element or the &lt;show/&gt; element, since these elements apply only to available resources. [Section 4.5.1, rfc3921bis-15]</p> <p>UC: &lt;presence type='unavailable'/&gt;</p> <p>NOTE: Optionally, the unavailable presence stanza MAY contain one or more &lt;status/&gt; elements specifying the reason why the user is no longer available.</p>  | 5.7.3.14.4.1  | R                           |
| 75 | <p>The user's server SHALL NOT depend on receiving unavailable presence from an available resource, since the resource can become unavailable ungracefully (e.g., the resource can be timed out by the server because of inactivity). [Section 4.5.2, rfc3921bis-15]</p> <p>If an available resource becomes unavailable for any reason (either gracefully or ungracefully), the user's server SHALL broadcast unavailable presence to all contacts that meet all of the following criteria [Section 4.5.2, rfc3921bis-15]:</p> <ul style="list-style-type: none"> <li>a. The contact is in the user's roster with a subscription type of "from" or "both".</li> <li>b. The last presence stanza received from the contact during the user's presence session was not of type "error" or "unsubscribe".</li> </ul> <p>If the unavailable notification was gracefully received from the client, then the server SHALL broadcast the full XML of the presence stanza. [Section 4.5.2, rfc3921bis-15]</p> <p>The user's server SHALL also send the unavailable notification to all of the user's available resources (including the resource that generated the presence notification in the first place). [Section 4.5.2, rfc3921bis-15]</p> <p>If the server detects that the user has gone offline ungracefully, then the server SHALL generate the unavailable presence broadcast on the user's behalf. [Section 4.5.2, rfc3921bis-15]</p> | 5.7.3.14.4.2  | R                           |
| 76 | Upon receiving an unavailable notification from the user, the contact's server SHALL deliver the user's presence stanza to all of the contact's available resources. [Section 4.5.3, rfc3921bis-15]   | 5.7.3.14.4.3  | R                           |
| 77 | From the perspective of the contact's client, there is no significant difference between initial presence broadcast and unavailable presence broadcast, so the contact's client SHALL follow the rules for processing of inbound presence defined under Section 5.7.3.14.1.4, Client Processing of Inbound Initial Presence. [Section 4.5.4, rfc3921bis-15]   | 5.7.3.14.4.4  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement  | UCR Reference | Required (R) Conditions (C) |
|----|--|---------------|-----------------------------|
| 78 | <p>To specify a particular availability sub-state, a client implementation SHALL support the &lt;show/&gt; element within a presence stanza. A presence stanza SHALL NOT contain more than one &lt;show/&gt; element. The XML character data of the &lt;show/&gt; element is not human-readable. The XML character data SHALL be one of the following [Section 4.7.2.1, rfc3921bis-15]:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> away – The entity or resource is temporarily away.</li> <li><input type="checkbox"/> chat – The entity or resource is actively interested in chatting.</li> <li><input type="checkbox"/> dnd – The entity or resource is busy (dnd = “Do Not Disturb”).</li> <li><input type="checkbox"/> xa – The entity or resource is away for an extended period (xa = “eXtended Away”).</li> </ul> <p>NOTE: If no &lt;show/&gt; element is provided, the entity is assumed to be online and available. [Section 4.7.2.1, rfc3921bis-15]</p> <p>NOTE: While support for this feature is required, the use of this feature is optional.</p> | 5.7.3.14.5.1  | R                           |
| 79 | <p>To convey human-readable XML character data specifying a natural-language description of an entity’s availability, the client SHALL support the &lt;status/&gt; element within a presence stanza. It is normally used in conjunction with the show element to provide a detailed description of an availability state (e.g., “In a meeting”) when the presence stanza has no ‘type’ attribute. There are no attributes defined for the &lt;status/&gt; element, with the exception of the ‘xml:lang’ attribute. [Section 4.7.2.2, rfc3921bis-15]</p> <pre>&lt;presence from='john.smith@chat1.dod.mil/office' xml:lang='en'&gt; &lt;show&gt;dnd&lt;/show&gt; &lt;status&gt;In a meeting&lt;/status&gt; &lt;/presence&gt;</pre> <p>NOTE: A presence stanza of type “unavailable” MAY also include a &lt;status/&gt; element to provide detailed information about why the entity is going offline.</p> <p>NOTE: While support for this feature is required, the use of this feature is optional.</p>   | 5.7.3.14.5.2  | O                           |
| 80 | <p>The OPTIONAL &lt;priority/&gt; element contains non-human-readable XML character data that specifies the priority level of the resource. The value SHALL be an integer between -128 and +127. [Section 4.7.2.3, rfc3921bis-15]</p> <pre>&lt;presence xml:lang='en'&gt; &lt;show&gt;dnd&lt;/show&gt; &lt;status&gt;In Meeting&lt;/status&gt; &lt;priority&gt;1&lt;/priority&gt; &lt;/presence&gt;</pre> <p>If no priority is provided, the processing server or client SHOULD consider the priority to be zero (“0”).</p>  | 5.7.3.14.5.3  | O                           |
| 81 | <p>When a user’s client is engaged in a chat session with a contact, the user’s client SHALL send a message of type “chat” and the contact’s client SHALL preserve that message type in subsequent replies. [Section 5.1, rfc3921bis-15]</p> <p>The user’s client SHALL be capable of including a &lt;thread/&gt; element with its initial message, which the contact’s client SHALL also preserve during the life of the chat session. The primary use of the XMPP &lt;thread/&gt; element is to uniquely identify a conversation thread or “chat session” between two entities instantiated by &lt;message/&gt; stanzas of type ‘chat’. [Section 5.1, rfc3921bis-15]</p>   | 5.7.3.15.1    | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

| ID | Requirement   | UCR Reference | Required (R) Conditions (C) |
|----|---|---------------|-----------------------------|
| 81 | The user's client SHALL address the initial message in a chat session to the bare JID of the contact (i.e., <contact@domain>). Until and unless the user's client receives a reply from the contact, it SHALL continue sending any further messages to the contact's bare JID. Once the user's client receives a reply from the contact's full JID, it SHALL address its subsequent messages to the contact's full JID as provided in the 'from' address of the contact's replies. [Section 5.1, rfc3921bis-15]   | 5.7.3.15.1    | R                           |
|    | The contact's client SHALL address its subsequent replies to the user's full JID <user@domain/resource> as provided in the 'from' address of the initial message. [Section 5.1, rfc3921bis-15]  |               |                             |
| 82 | An instant messaging client SHALL specify the intended recipient for a message stanza by providing the JID of the intended recipient in the 'to' attribute of the <message/> stanza. [Section 5.2.1, rfc3921bis-15]   | 5.7.3.15.2.1  | R                           |
| 83 | An instant messaging client SHALL support all of the following message types [Section 5.2.2, rfc3921bis-15]:<br><br>a. chat – The value "chat" indicates that the message is sent in the context of a one-to-one chat session. Typically a receiving client will present/display messages of type "chat" in an interface that enables one-to-one chat between the two parties, including an appropriate conversation history.<br><br>b. error – The value "error" indicates that the message is generated by an entity that experienced an error in processing a message received from another entity.<br><br>NOTE: A client that receives a message of type "error" SHOULD present an appropriate interface informing the sender of the nature of the error.<br><br>c. groupchat – The value "groupchat" indicates that the message is sent in the context of a multiuser chat environment. Typically, a receiving client will present a message of type "groupchat" in an interface that enables many-to-many chat between the parties.<br><br>d. normal – The value "normal" indicates that the message is a standalone message that is sent outside the context of a one-to-one conversation or groupchat, and to which it is expected that the recipient will reply. Typically, a receiving client will present a message of type "normal" in an interface that enables the recipient to reply, but without a conversation history. The default value of the 'type' attribute is "normal".<br><br>NOTE: Support for the following message type is defined as recommended.<br><br>e. headline – The value "headline" indicates that the message provides an alert, a notification, or other information to which no reply is expected (e.g., news headlines, sports updates, near-real-time market data, and syndicated content). Because no reply to the message is expected, typically a receiving client will present a message of type "headline" in an interface that appropriately differentiates the message from standalone messages, chat messages, or groupchat messages (e.g., by not providing the recipient with the ability to reply).<br><br>If an application receives a message with no 'type' attribute or the application does not understand the value of the 'type' attribute provided, it SHALL consider the message to be of type "normal" (i.e., "normal" is the default). [Section 5.2.2, rfc3921bis-15] | 5.7.3.15.2.2  | R                           |
|    |   |               |                             |
| 84 | A client SHALL be capable of populating a <message/> stanza with the <body/> element. The <body/> element contains human-readable XML character data that specifies the textual content of the message.<br><br>NOTE: While support for this feature is required, the use of this feature is optional. This child element is normally included in a message stanza. [Section 5.2.3, rfc3921bis-15]<br><br>NOTE: There are no attributes defined for the <body/> element, with the exception of the 'xml:lang' attribute. Multiple instances of the <body/> element MAY be included in a message stanza, but only if each instance possesses an 'xml:lang' attribute with a distinct language value. [Section 5.2.3, rfc3921bis-15]   | 5.7.3.15.2.3  | R                           |

**Table 3-1. XMPP Capability/Functional Requirements (continued)**

|                |   |       |  |
|----------------|---|-------|--|
| <b>LEGEND:</b> |   |       |  |
| AF             | Assured Forwarding  | IS-IS | Intermediate System-Intermediate System  |
| AR             | Aggregation Router  | ITU-T | International Telecommunication Union - Telecommunication Standardization Sector |
| ASLAN          | Assured Services Local Area Network                         |       |  |
| BGP            | Border Gateway Protocol                                     | JID   | Jabber IDentification  |
| B/P/C/S        | Base/Post/Camp/Station                                      | Mbps  | Megabits per second  |
| C              | Conditional   | MFS   | Multifunction Switch   |
| CER            | Customer Edge Router  | MFSS  | Multifunction Softswitch   |
| CM             | Configuration Management                                    | MIB   | Management Information Base  |
| DiffServ       | Differentiated Services                                     | MPLS  | Multiprotocol Label Switching  |
| DISA           | Defense Information Systems Agency                          | ms    | millisecond  |
| DISN           | Defense Information System Network                          | MTU   | Maximum Transmission Unit  |
| DS1            | Digital Signal Level 1 (1.544 Mbps)                         | NM    | Network Management   |
| DS3            | Digital Signal Level 3                                      | NMS   | Network Management System  |
| DSCP           | Differentiated Services Code Point                          | OSPF  | Open Shortest Path First   |
| E1             | European Basic Multiplex Rate (2.048 Mbps)                  | para  | paragraph  |
| E2E            | End-to-End  | PE    | Provider Edge  |
| EBC            | Edge Boundary Controller                                    | PHB   | Per Hop Behavior   |
| EF             | Expedited Forwarding  | PM    | Performance Management   |
| EI             | End Instrument  | QoS   | Quality of Service   |
| EO             | End Office  | R     | Required   |
| F-F            | Fixed-to-Fixed  | RFCs  | Request for Comments   |
| FCAPS          | Fault, Configuration, Accounting, Performance, and Security | SQF   | System Quality Factors   |
| FO-F           | FLASH OVERRIDE/FLASH  | SUT   | System Under Test  |
| FRR            | Fast Re-Route   | T1    | Digital Transmission Link Level 1 (1.544 Mbps)                                   |
| GEI            | Generic End Instrument                                      | TDM   | Time Division Multiplexing   |
| GOS            | Grade of Service  | TLS   | Transport Layer Security   |
| I/P            | IMMEDIATE/PRIORITY  | UC    | Unified Capabilities   |
| IAW            | in accordance with  | VLAN  | Virtual Local Area Network   |
| IEEE           | Institute of Electrical and Electronics Engineers           | VVoIP | Voice and Video over Internet Protocol   |
| IP             | Internet Protocol   | WAN   | Wide Area Network  |
| IPv4           | Internet Protocol version 4                                 | XML   | Extensible Mark-up Language  |
| IPv6           | Internet Protocol version 6                                 | XMPP  | Extensible Mark-up and Presence Protocol   |